FL MGUARD 1000
Installation and startup

User manual

UM EN FL MGUARD 1000

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

FL MGUARD 1000 – Installation and startup

UM EN FL MGUARD 1000, Revision 11 2024-05-16

This user manual is valid for:

Designation	Version	Order No.
FL MGUARD 1102		1153079
FL MGUARD 1105		1153078

For further information see *mGuardNT 1.8.x firmware Release Notes*.

108413_en_11

PHOENIX CONTACT GmbH & Co. KG • Flachsmarktstraße 8 • 32825 Blomberg • Germany
phoenixcontact.com

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 1000 series are security routers for industrial use, with integrated stateful packet inspection firewall. They are suitable for distributed protection of production cells or individual machines against manipulation.

– The devices are intended for installation in a control cabinet.

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

This module snaps onto a DIN rail inside a control cabinet or control box. This control cabinet/box must meet the requirements of IEC/EN 62368-1with respect to fire protection enclosure.

NOTE: Requirement for functional grounding

Mount the module 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 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.

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.
- 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.

1.7 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 2024-04-15; 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.

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/products.

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 describes in the „FL MGUARD 1000 – Web based management“ (UM ENMGUARD NT) user manual, available in the „Download“ area at phoenixcontact.net/product/1153079.

2 Device description

The devices of the FL MGUARD 1000 series are security routers for industrial use, with integrated stateful packet inspection firewall. They provide high data throughput and are suitable for distributed protection of production cells or individual machines against manipulation.

NAT router

As a router or gateway, the device connects subnets or network zones. A separate IP address is configured for each network zone, via which the device can be reached in the network.

Using the NAT functionality (IP masquerading, 1:1 NAT, Port forwarding), separate machines (PLCs) or multiple subnets with the same IP configuration can easily be integrated into an existing network without having to change the IP configuration of the machine or the subnets.

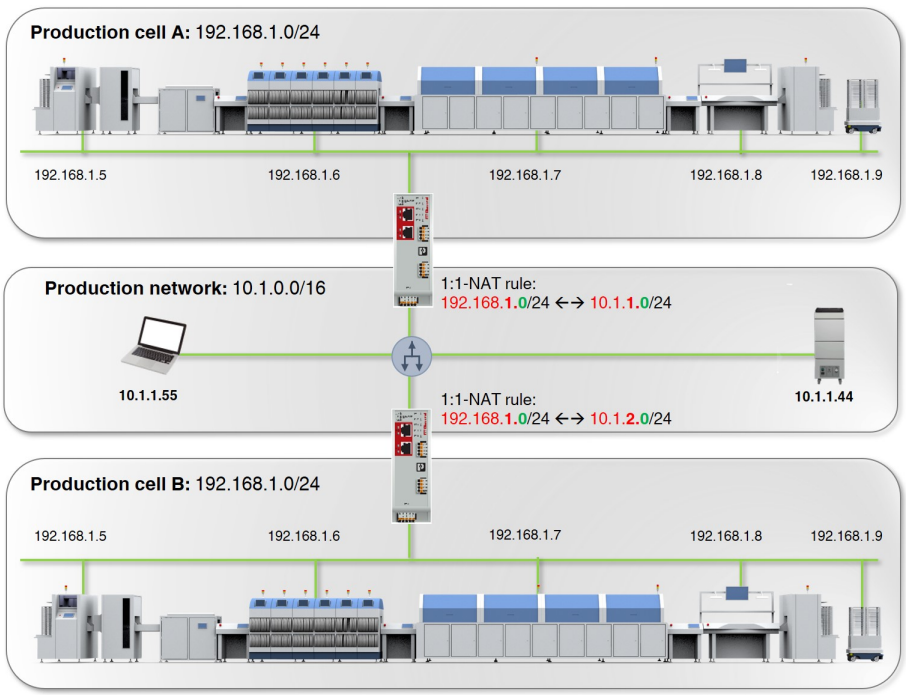


Figure 2-1 NAT router

Security by Design

All mGuard devices feature the proven mGuard Security Technology and have thus been designed from the ground up to meet network security requirements. The devices use a powerful firewall. System and network services have been hardened.

Vulnerabilities - quickly closed (PSIRT)

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

Thanks to the integrated mGuard Security Technology, the devices provide decentralized protection of production cells or individual machines against manipulation.

2.1 Product overview

Table 2-1 Product overview and order numbers

Device	Short description	Order No.
FL MGUARD 1102	2 x RJ45 ports, SD card holder, digital service I/Os	1153079
FL MGUARD 1105	5 x RJ45 ports, SD card holder, digital service I/Os	1153078

2.2 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.

2.2.1 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.
- Submit claims for any transport damage immediately, and inform Phoenix Contact or your supplier as well as the shipping company without delay.
- Enclose photos clearly documenting 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 6.

2.3 FL MGUARD 1102

The device provides the following network connections:

– **Network interface 1 / Net zone 1**: Ethernet 10/100/1000 Mbps (RJ45 port)
– **Network interface 2 / Net zone 2**: Ethernet 10/100/1000 Mbps (RJ45 port)

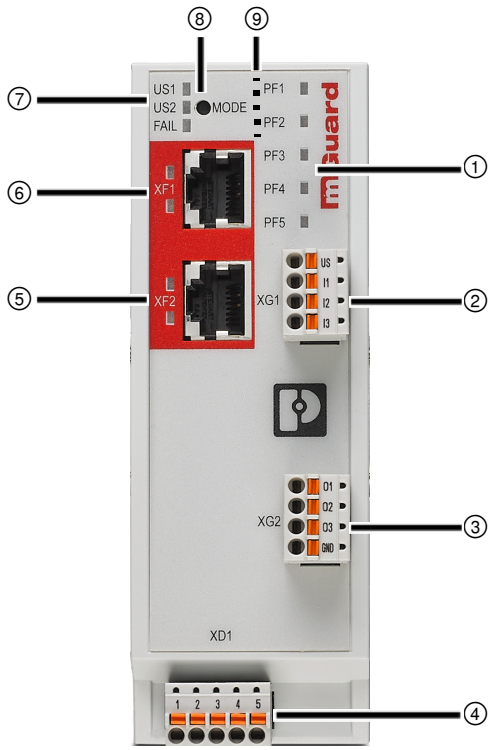


Figure 2-2 FL MGUARD 1102 operating elements and LEDs

① Status and diagnostic LEDs
(See Section 2.5.1)

② Connection of digital **inputs** via COMBICON connector (Push-in contact)
(See Section 3.4)

③ Connection of digital **outputs** via COMBICON connector (Push-in contact)
(See Section 3.4)

④ Connection of supply voltage via COMBICON connector (Push-in contact)
(See Section 3.2)

⑤ Network interface 2 / Net zone 2 (RJ45 Ethernet port) (see Section 3.3)
LNK/ACT LED (top) I SPD LED (bottom)
(see Section 2.5.2)

⑥ Network interface 1 / Net zone 1 (RJ45 Ethernet port) (see Section 3.3)
LNK/ACT LED (top) I SPD LED (bottom)
(see Section 2.5.2)

⑦ Status and diagnostic LEDs
(See Section 2.5.3, 2.5.4)

⑧ Mode button
(See Section 5)

⑨ SD card holder (on the back of the device)
(See Section 3.5)

2.4 FL MGUARD 1105

The device provides the following network connections:

– **Network interface 1 / Net zone 1**: Ethernet 10/100/1000 Mbps (RJ45 port)
– **Network interface 2 / Net zone 2**: Ethernet 10/100/1000 Mbps (RJ45 port)

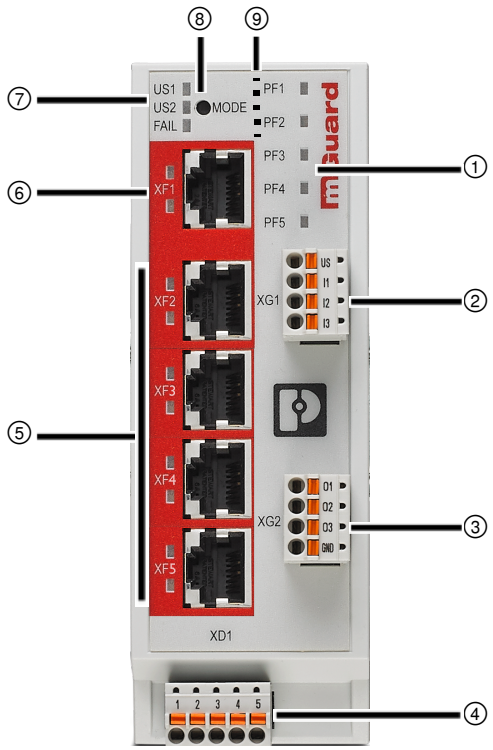


Figure 2-3 FL MGUARD 1105 operating elements and LEDs

① Status and diagnostic LEDs
(See Section 2.5.1)

② Connection of digital **inputs** via COMBICON connector (Push-in contact)
(See Section 3.4)

③ Connection of digital **outputs** via COMBICON connector (Push-in contact)
(See Section 3.4)

④ Connection of supply voltage via COMBICON connector (Push-in contact)
(See Section 3.2)

⑤ Network interface 2 / Net zone 2 (RJ45 Ethernet port) (see Section 3.3)
LNK/ACT LED (top) I SPD LED (bottom)
(see Section 2.5.2)

⑥ Network interface 1 / Net zone 1 (RJ45 Ethernet port) (see Section 3.3)
LNK/ACT LED (top) I SPD LED (bottom)
(see Section 2.5.2)

⑦ Status and diagnostic LEDs
(See Section 2.5.3, 2.5.4)

⑧ Mode button
(See Section 5)

⑨ SD card holder (on the back of the device)
(See Section 3.5)

2.5 LED status and diagnostic indicators

The status and diagnostic LEDs indicate different system and error states of the device.

2.5.1 PF1-PF5

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

They are used during operation in *Smart Mode*, for example (see Table 2-3).

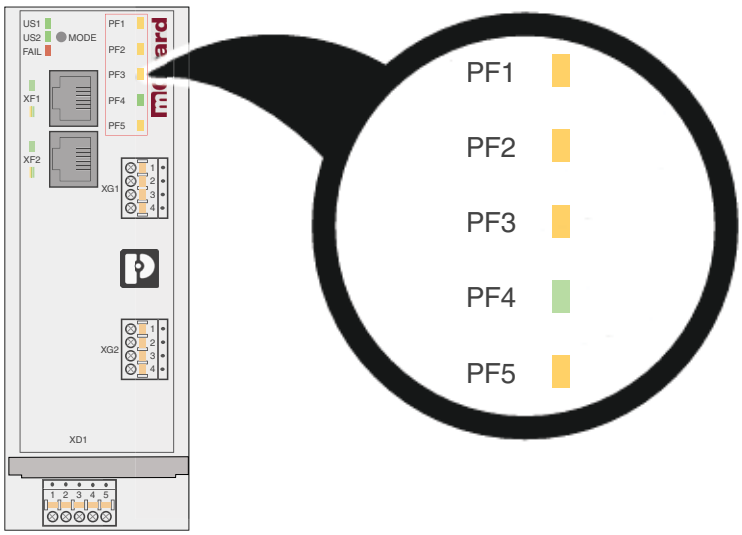


Figure 2-4 LEDs: PF1-PF5

Table 2-2 LEDs: PF1 – PF5: Device status

Device status				Device error
Is being started	**Firmware update**	**Ready for operation**	**Test mode alarm**	**Import from SD card failed**
PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5
Wait until the device has been started up completely.	The firmware is written to the device. **NOTE: An interruption in the power supply can damage the device!** **Do not switch off the device!** Wait until the device has been started up completely.	The device has been started up completely. The PF1 LED flashes with the rhythm of a heartbeat.	The firewall test mode is active and has triggered one or several alarms. The PF1 LED flashes with the rhythm of a heartbeat.	The attempt to load a configuration from SD card into the device and apply it failed. The device is started with the factory settings. The FAIL LED also lights up permanently red.

Table 2-3 LEDs: PF1 – PF5: *Smart Mode*

„Smart mode“ function (see Section 5.1)			
Selected (example)	**Is being executed** (example)	**Completed successfully**	**Failed**
PF1 PF2 **PF3** PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5
The LED shows which *Smart mode* function has been selected (see Table 5-1). Additionally, PF1–5 flash green simultaneously three times every four seconds.	The *Smart mode* function is executed. Do not switch off the device. **NOTE: An interruption in the power supply can damage the device!** **Do not switch off the device!** Wait until the *Smart mode* function has been completed successfully.	The *Smart mode* function has been executed successfully. Restart the device.	In the event of an error, restart the device. If the error persists, contact your support. A severe error can also be indicated by the “FAIL” LED.

2.5.2 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 Table 2-4).

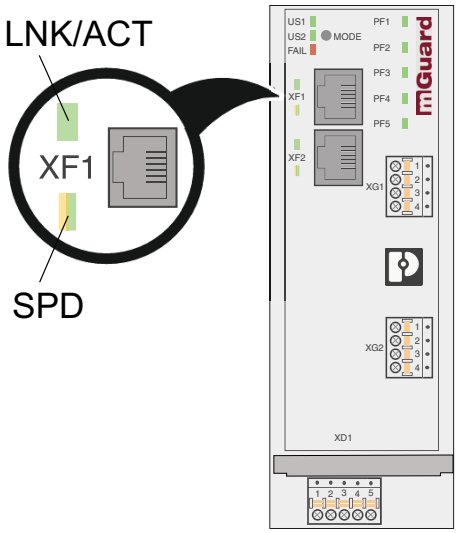


Figure 2-5 LEDs: LNK/ACT and SPD

Table 2-4 LEDs: 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)
		Off	No data transmission (if LNK/ACT LED is inactive)

2.5.3 US1 and US2

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

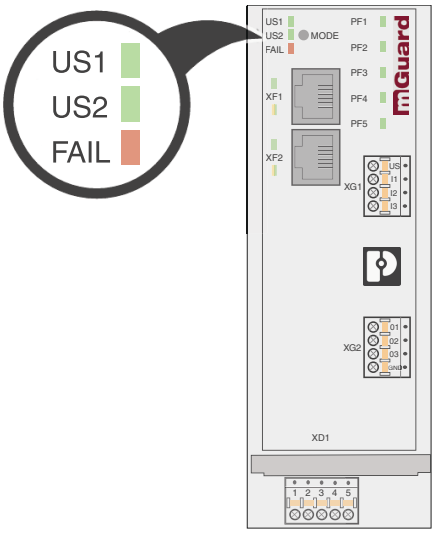


Figure 2-6 LEDs: US1, US2

Table 2-5 LEDs: US1, US2

Designation	Color	Status	Meaning
US1	Green	On	Supply voltage within the tolerance range (see Section 7)
		Off	Supply voltage not present or too low (see Section 7)
US2	Green	On	The devices do not have a redundant power supply.
		Off	

2.5.4 FAIL

The FAIL LED indicates different states and error states of the device.

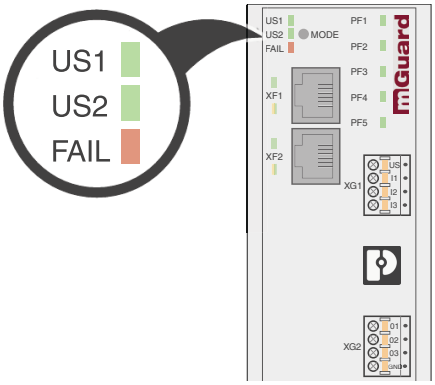


Figure 2-7 LED: FAIL

Table 2-6 LED: FAIL

Designation	Color	Status	Meaning
FAIL	Red	On (briefly)	The device restarts. • Wait until the device is ready to operate (see Section 4.3.1). ⇒ The device is ready to operate when PF2–PF5 have gone out and PF1 flashes green (heartbeat).
		On (permanent)	A serious error occurred. ⇒ The device did not reach readiness for operation. ⇒ All network interfaces have been deactivated. • Restart the device.
		On (permanent) + LED PF1 (red)	The PF1 LED also lights up permanently red. ⇒ The attempt to load a configuration from SD card into the device and apply it failed. ⇒ The device is started with the factory setting.
		On (blinking)	A serious error occurred. ⇒ The device did not reach readiness for operation. ⇒ All network interfaces have been deactivated. • Restart the device.
		Contact your support, if necessary (see Section 1.9).	

2.6 Factory settings

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

2.6.1 Network interfaces

The basic network functions (Ethernet) of the device are available after the device start (see Table 2-7).

Table 2-7 **Factory settings**: configuration of the network interfaces

Function	Net zone 1 (XF1)	Net zone 2 (XF2–XF5) (*bridge mode*)
IP address (IPv4)	If there is a DHCP server in the network, the IP address is assigned automatically.	192.168.1.1
Net mask		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 (downstream of net zone 1).	–

2.6.2 User access

The WBM and *Config API* user interfaces can be accessed by entering user name and password.

– **User name**: *admin*
– **Password** *private*

During the initial device startup, immediately change the preset administrator password.

Additionally, network access to the device is restricted by the firewall for incoming data traffic (see “Firewall (for incoming data traffic) = device access”).

2.6.3 Active network services (device as client)

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

Table 2-8 **Factory settings**: active services (as client)

Service	Active via	Configuration (factory settings)
DHCP client	Net zone 1 (XF1)	Sends DHCP requests to available DHCP servers in its network via UDP port 67.
DNS client	Net zone 1 (XF1) (Net zone 2 [XF2–XF5] applies the settings of net zone 1)	Sends DNS requests to available DNS servers via UDP port 53. Factory settings: The address of a DNS server can be assigned per DHCP if there is a DHCP server in the network. If no address has been assigned via DHCP, the *root name server* preset in the device is used.
NTP client	Net zone 1 (XF1) Net zone 2 (XF2–XF5)	Sends NTP requests to available NTP servers via UDP port 123. Factory settings: The following addresses (host names) of the NTP server have been preset: – 0.pool.ntp.org – 1.pool.ntp.org – 2.pool.ntp.org – 3.pool.ntp.org

2.6.4 Active network services (device as server)

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

Table 2-9 **Factory setting**: active services (as server)

Service	Accessible via	Configuration (factory settings)
Web server	Net zone 2 (XF2–XF5)	Request via TCP-Port 443 (HTTPS) Clients that are connected with the device via net zone 2 can access the web-based management (WBM).
RESTful server	Net zone 2 (XF2–XF5)	Request via TCP-Port 443 (HTTPS) Clients that are connected with the device via net zone 2 can access the RESTful server (*Config API*).
SNMP server	Net zone 2 (XF2–XF5)	Request via UDP-Port 161 (SNMP) Clients that are connected with the device via net zone 2 can access the SNMP server (*read only*).
DHCP server	Net zone 2 (XF2–XF5)	Request via UDP port 67 Clients that are connected with the device via net zone 2 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 server: 192.168.1.1
DNS server	Net zone 2 (XF2–XF5)	Request via UDP and TCP port 53 Clients that are connected with the device via net zone 2 can send name resolution requests to its DNS server.
NTP server	Net zone 2 (XF2–XF5)	Request via UDP port 123 Clients that are connected with the device via net zone 2 can synchronize their system time via the NTP server of the device.

2.6.5 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 (device access).
– **Routed data traffic** is the packets that are *routed* through the device, for example that come in via net zone 2 (XF2–XF5) and go out via net zone 1 (XF1).

Firewall (for incoming data traffic) = device access

Factory settings: firewall for incoming data traffic

Service, protocol	Incoming via	Port	Description
HTTPS	Net zone 2 (XF2–XF5)	TCP 443	Corresponding requests to the web server of the device are permitted, i.e.: – login and configuration via web-based management – login and configuration via RESTful server (*Config API*)
SNMP	Net zone 2 (XF2–XF5)	UDP 161	Corresponding requests to the SNMP server of the device are permitted.
DHCP	Net zone 2 (XF2–XF5)	UDP 67	Corresponding requests to the DHCP server of the device are permitted.
DNS	Net zone 2 (XF2–XF5)	TCP 53 UDP 53	Corresponding requests to the DNS server of the device are permitted.
NTP	Net zone 2 (XF2–XF5)	UDP 123	Corresponding requests to the NTP server of the device are permitted.
ICMP (IPv4)	Net zone 2 (XF2–XF5)		Ping requests (*ICMP requests*) to the configured or assigned (per DHCP) IPv4 addresses of the net zones (in *router mode*) or the management IP address (in *stealth mode*) are permitted.

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

Factory settings: Firewall (for routed data traffic) = routing
All packets that are sent from net zone 2 (XF2–XF5), i.e. from subnetwork 192.168.1.0/24, to any target address are forwarded by the device (*routed*).
(Rule: 192.168.1.0/24 --> 0.0.0.0/0 = ACCEPT).
All other packets are rejected.

3 Mounting and installation

3.1 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.

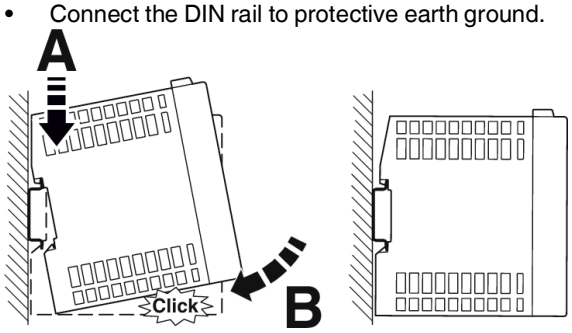


Figure 3-1 Snapping the device onto a DIN rail

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**).

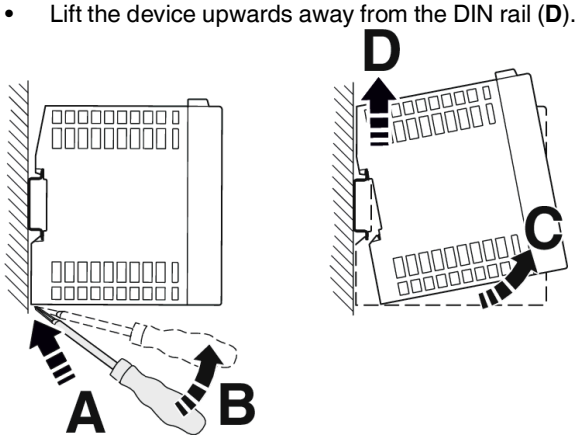


Figure 3-2 Removing the device

3.2 Connecting the supply voltage

NOTE: Electrical voltage
The device is designed exclusively for operation with safety extra-low voltage (SELV/PELV) in accordance with EN/IEC 62368-1. The device may only be connected to devices that meet the requirements of EN/IEC 62368-1. Provide overcurrent protection (I ≤ 5 A) in the installation.

The device is operated using a 24 V DC voltage.

Table 3-1 Power supply via COMBICON connector

COMBICON	1	2	3	4	5
XD1	**US1**	**GND**	**Not available**		**Functional ground**
1 2 3 4 5 US1 GND FE	18...36 V	0 V	**N/A**	**N/A**	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 3-1).
- Plug COMBICON connector **XD1** onto the device.

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

3.2.1 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**.

3.3 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.

3.3.1 Using RJ45 Ethernet connectors

Table 3-2 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 3-2).
- 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.

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

NOTE: External voltage source
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.

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 3-3).

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.

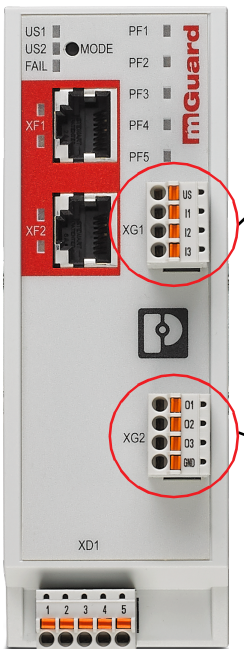


Table 3-3 **Input I1-3**: service contacts via COMBICON connector

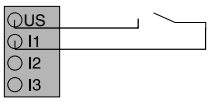
COMBICON XG1	Input (I1–3)		Example
	**US**	Voltage output (**US**) (+) (short-circuit-proof)	
	I1	Switching inputs **(I1–3)**	
	I2		
	I3		

Table 3-4 **Output O1–3**: Service contacts via COMBICON connector

COMBICON XG2	Output (O1–3)		Example
	**O1**	Switching outputs (**O1–3**)	
	O2	Short-circuit-proof switching output (24 V DC)	
	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 18 ... 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 3-3 and 3-4).
- Plug COMBICON connector **XG1** or **XG2** onto the device.

3.5 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).

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

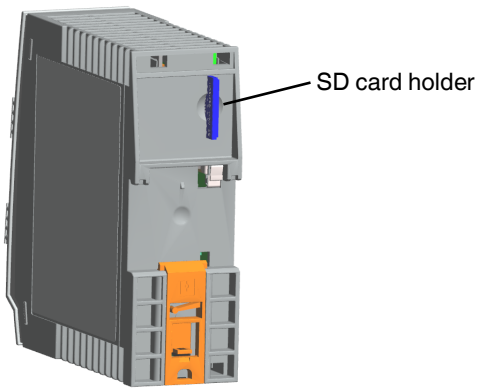


Figure 3-3 SD card holder on the back of the device

4 Initial startup

The initial startup for the device can be performed in *Easy Protect Mode* or in *Router mode*.

Easy Protect Mode (see Section 4.2)

- The device is invisibly integrated into an existing network.
- It is neither necessary nor possible to configure the device.
- The firewall of the device automatically protects all devices connected via network interface 2 (net zone 2 / XF2–XF5) against network access via network interface 1 (net zone 1 / XF1).
- Protected devices in net zone 2 (XF2–XF5) can access all devices in the network.

Router mode (see Section 4.3)

- 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 net zone 2 (XF2–XF5) can automatically obtain their IP configuration from the device per DHCP.
- The firewall of the device automatically protects all devices connected via net zone 2 against external network access from net zone 1 (XF1).
- Desirable external access to protected devices can be specifically permitted (firewall and NAT rules).
- The protected devices in net zone 2 can access all devices in both net zones.
- The protected devices in net zone 2 can access server services of the device (WBM, DHCP, DNS, NTP).

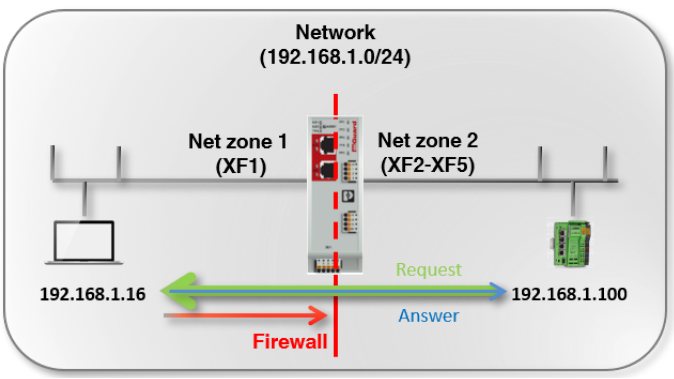
4.1 Required components

- Device with COMBICON connector (for XD1)
- 24 V power supply
- Network cable (Ethernet)
- Wire bridge (only *Easy Protect Mode*)
- Configuration computer (only *Router mode*)

4.2 Operating the device in “Easy Protect Mode”

If the device is operated in *Easy Protect Mode*, it **automatically** protects all devices connected via net zone 2 (XF2–XF5) against external access (e.g. individual machines or production cells that are connected via a switch).

The device is integrated into the existing network via its net zones 1 and 2 (XF1 and XF2–XF5) without changing the existing network configuration of the connected devices (see Figure 4-1).



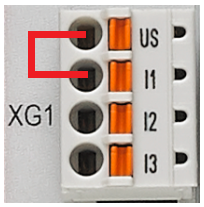


Figure 4-1 Operating the device in *Easy Protect Mode* (example configuration)

Network connections that are established by the protected devices (from net zone 2) are not blocked by the firewall.

The device itself does not have own IP addresses and is not detected as network device in the network.

It is generally neither necessary to configure the device, nor possible, due to the lack of access options via the web-based management (HTTPS).

In *Easy Protect Mode*, firmware updates can be performed via the *Smart Mode* function "Updating from SD card" (see Section 5.1.4).

Since security-relevant improvements are added to the product with each new firmware version, you should always update to 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 (e.g. phoenixcontact.net/product/1153079).

- 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.

4.2.1 Activating Easy Protect Mode

To operate the device in *Easy Protect Mode,* proceed as follows:

- Disconnect the device from the power supply.
- Bridge service contacts **US** and **I1** of the device (COMBICON connector **XG1**) with a cable bridge (see Figure 4-1 and Section 3.4).
- Connect the device with the voltage supply (see Section 3.2, “Connecting the supply voltage”).

⇒ The device is started and operated in active *Easy Protect Mode*.

4.2.2 Protecting network clients

- Connect the devices to be protected with **net zone 2** of the device via a network port (**XF2–XF5**).

  (To protect several devices, connect them to the device via an additional switch.)
- Connect the surrounding network to **net zone 1 (XF1)** via a switch

⇒ All network packets XF1 --> (XF2–XF5) are rejected.

⇒ All network packets (XF2–XF5) --> XF1 are accepted and forwarded.

4.3 Operating the device in router mode

If the device is operated in *router mode*, it acts as gateway between different subnets (see Figure 4-2).

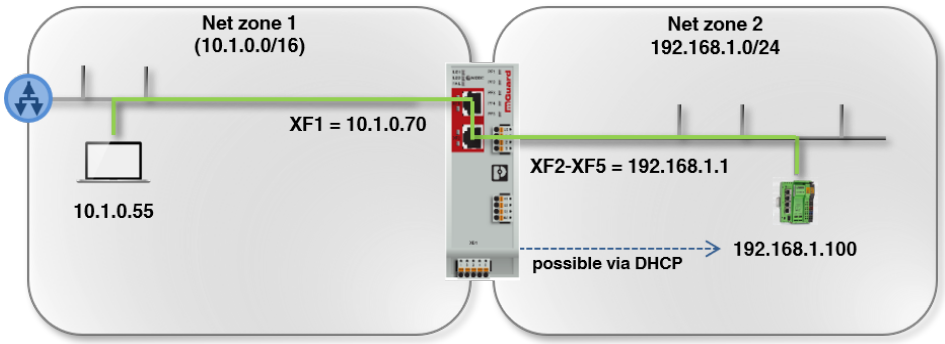


Figure 4-2 Operating the device in *router mode* (example configuration)

The data is *routed* between the two network interfaces (net zones) of the device.

In the factory settings, the data traffic from net zone 1 to net zone 2 is blocked by the firewall.

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

– 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 net zones can be enabled.

4.3.1 Starting the device

To start the device, proceed as follows:

• Connect the device with an external power supply (see Section 3.2, “Connecting the supply voltage”).

⇒ The device starts.

⇒ The FAIL LED briefly lights up in red.

⇒ During the boot process, the PF1–5 LEDs light up orange.

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

4.3.2 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 4-3).

Below, configuration of the device via net zone 2 (XF2–XF5) is described. (In factory settings, the configuration via net zone 1 is not possible.)

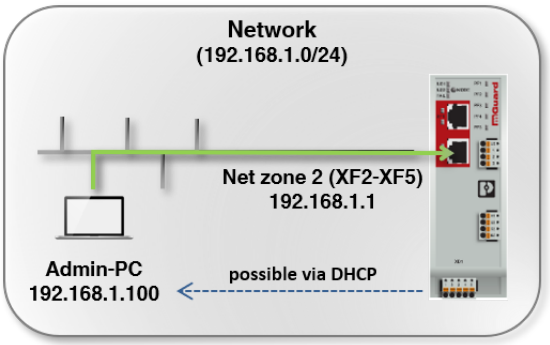


Figure 4-3 Establishing a network connection to the device

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 4-1.

Table 4-1 IP configuration (example): establishing a network connection

Device	IP	Net mask	Gateway
Device (Factory settings for XF2–XF5)	192.168.1.1	24 (255.255.255.0)	-
Configuration computer (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 XF2–XF5 of net zone 2 of the device (see Figure 4-3).
- 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 net zone 2 (XF2–XF5).

Checking the IP configuration

- 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

To automatically obtain the IP setting of the configuration computer, proceed as follows;

- 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)*".

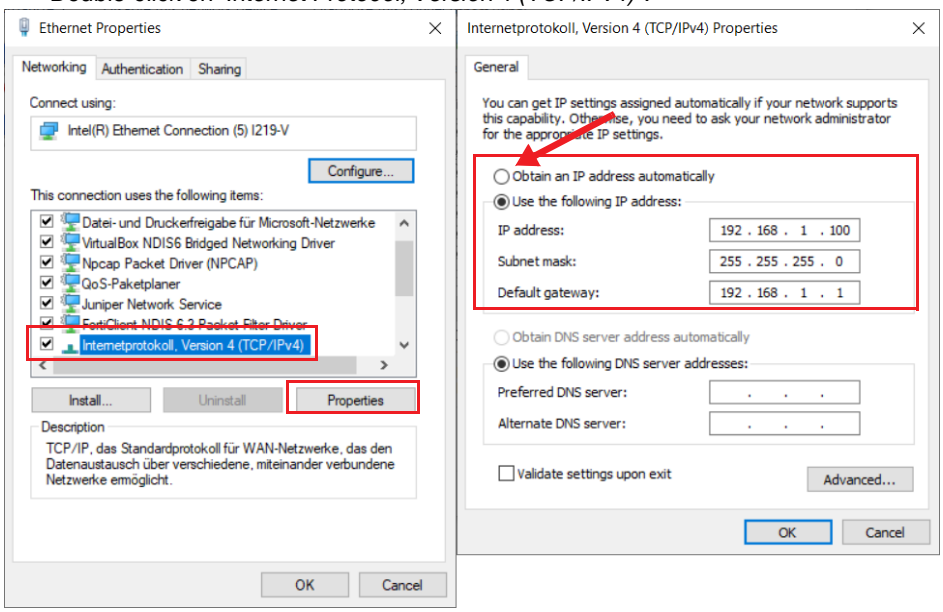


Figure 4-4 Changing the IP setting of the configuration computer (admin PC)

- 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 4-4 / Table 4-1.
- Confirm with "*OK*".

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

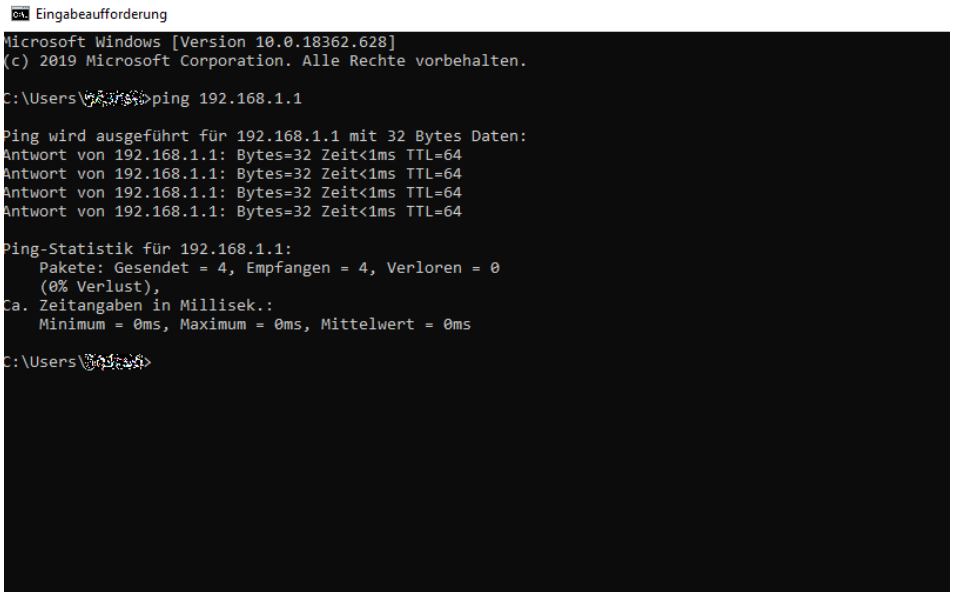
⇒ The device serves as default gateway for the configuration computer.

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.



4.4 Commissioning the device with a saved configuration from SD card

Using the "External configuration storage (ECS)" function, it is possible to save the current device configuration on an SD card (see "UM EN MGUARD NT" user manual, available at phoenixcontact.net/product/1153079).

A configuration saved on SD card can be imported into a new device.

This makes it possible to carry out a device exchange quickly and easily if a malfunction should ever occur in a device.

Furthermore, new devices can easily be commissioned based on an existing configuration.

Prerequisite: Firmware version "SD card" is lower/equal to firmware version "Device".

Proceed as follows:

- Use a brand new device or a device where the factory settings have been restored using *Smart Mode* (see Section 5.1.3).
- Insert the SD card with the saved configuration into the SD card holder. The three files *users_pass.json, snmp-pass.conf* and *configuration.json* must be available on the SD card (individually or packed as *mGuard.tar.gz*: the individual files are used with priority).
- Start the device.

⇒ The configuration is automatically imported from the SD card to the device and applied there.

⇒ If an error occurs, the FAIL and PF1 LEDs light up red.

4.5 Using web-based management

4.5.1 Supported web browsers

The current versions of the following web browsers are supported:

– *Mozilla Firefox, Google Chrome, Microsoft Edge*

4.5.2 Supported users

Only the *admin* user can log on to the device.

The *admin* user has functionally unrestricted access to the web-based management (WBM) and the RESTful Configuration API (*Config API*) of the device.

4.5.3 Logging in to the device

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

- Connect the configuration computer with the device (see Section 4.3.2).
- Start a web browser on the configuration computer.
- Enter the IP address of the connected network interface of the device into 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.

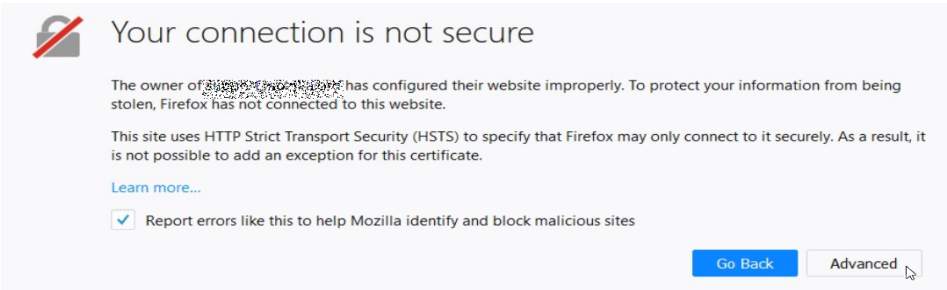


Figure 4-5 Certificate warning (Firefox)

- 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 the web-based management opens.

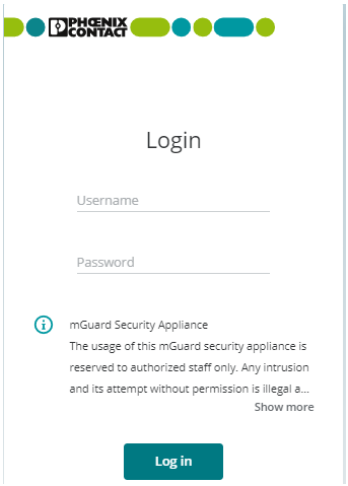


Figure 4-6 Login page of the web-based management

- Log in with the *admin* user name and the associated administrator password (factory settings: *private*).

⇒ The start page for the web-based management of mGuardNT opens.

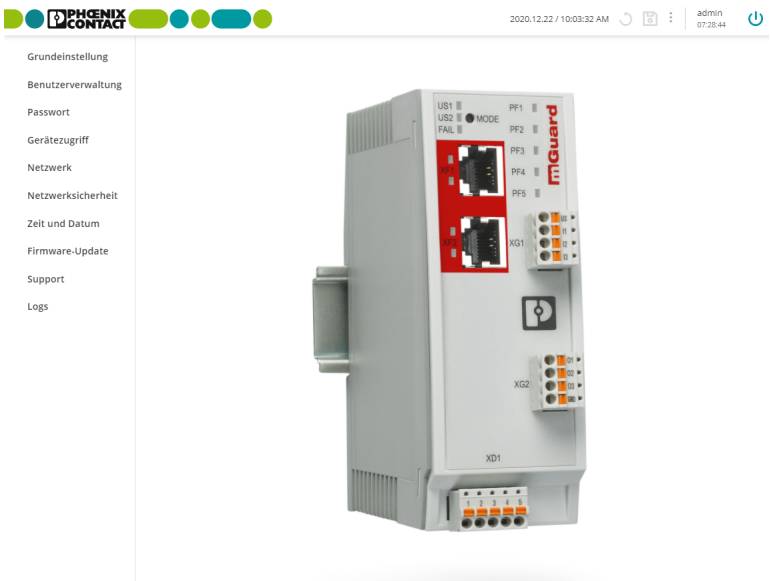


Figure 4-7 Start page for web-based management

The functions that can be configured by means of the web-based management are described in the "*FL MGUARD 1000 – Web-based management*" (UM EN MGUARD NT) user manual.

Available in the download area of the respective product page in the Phoenix Contact webshop, e.g. under phoenixcontact.net/product/1153079.

4.6 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(see "UM EN MGUARD NT" user manual, available at phoenixcontact.net/product/1153079)

Pressing the Mode button

• Press the Mode button for at least 5°seconds.
⇒ The FAIL LED lights up red.
• Release the Mode button.
⇒ The device restarts.
⇒ The PF1–5 LEDs light up orange.
⇒ The device is ready for operation when the PF1 LED flashes green (heartbeat).

Interrupting the power supply

• Briefly interrupt the power supply of the device.
⇒ The device restarts.
⇒ The PF1–5 LEDs light up orange.
⇒ The device is ready for operation when the PF1 LED flashes green (heartbeat).

Via web based management

• Open the menu: **Management >> System**
• Click the **Reboot** button to reboot the device.

4.7 Using the RESTful Configuration API

How to use the *Config API* is described in the "*FL MGUARD 1000 – RESTful Configuration API*" (UM EN MGUARD NT CONFIG API) user manual.
Available in the download area of the respective product page in the Phoenix Contact webshop, e.g. under phoenixcontact.net/product/1153079.

For experienced users only

In addition to configuration via the web-based management, the device can also be configured via the RESTful Configuration API (in short: *Config API*).

The *Config API* is provided via a RESTful web server of the device.

The data is transmitted via the HTTP(S) protocol, which is also used to call up websites.

5 Smart mode

With the *Smart Mode*, you can call up device functions without having access to a management interface of the device. Four *Smart Mode* functions are available.

– "Exiting without changes (PF1)"
– "Restoring configuration access (PF2)"
– "Restoring the factory settings (PF3)"
– "Updating from SD card (PF4)"

The Smart Mode function "PF5" is reserved exclusively for maintenance purposes and use by the manufacturer. Incorrect use can lead to irrevocable deletion of the device configuration.

5.1 Available „Smart mode“ functions

5.1.1 Exiting without changes (PF1)

Application

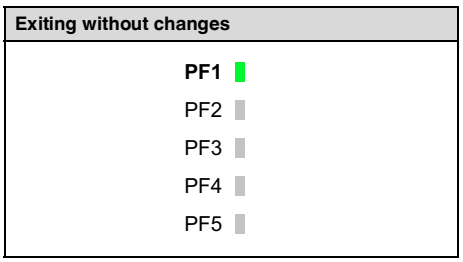
The user wants to exit *Smart Mode* without applying changes.

Result

– The device is restarted and boots the installed firmware version with the last configuration that was saved.
– All settings, passwords and certificates remain unaltered.

Execution

⇒ see "Using „Smart mode“" on page 47



5.1.2 Restoring configuration access (PF2)

Applications

– The IP configuration of the device is not known. It is therefore no longer possible to access the web-based management or the *Config API* of the device.
– The IP configuration of net zone 2 (XF2–XF5) is to be reset to the factory settings.

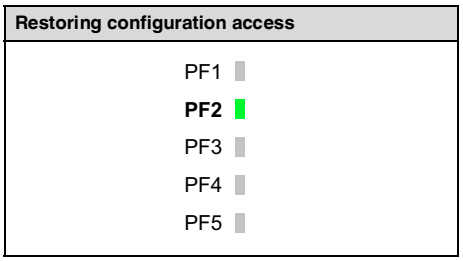
Result

Accessing the device via the default IP address is possible again:

– The default network configuration of net zone 2 (XF2–XF5) is restored: Mode: Router, IP address: 192.168.1.1, net mask: 24
– The default access rule for the web server (WBM) is restored for net zone 2 (see Section 2.6).
– The rest of the device configuration, users, passwords and certificates remain unaltered.

Execution

⇒ see “Using „Smart mode“” on page 47



5.1.3 Restoring the factory settings (PF3)

Applications

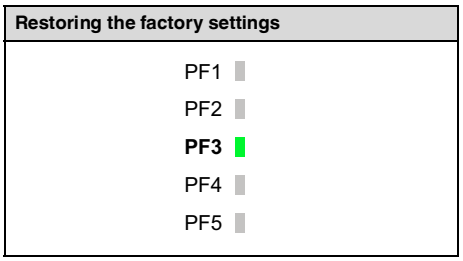
– The administrator password and other passwords are not known. It is therefore no longer possible to log on to the device.
– The device configuration, users, passwords and certificates are to be deleted securely and irretrievably.
– The device is to be taken out of operation.

Result

– The current device configuration, users, passwords and certificates are deleted securely and irretrievably.
– The device is reconfigured with the factory settings.

Execution

⇒ see “Using „Smart mode“” on page 47



5.1.4 Updating from SD card (PF4)

If the update via *Smart Mode* fails, please try to update the device via web-based management instead. If the update still fails, please refer to the error messages shown in the user interface or in the log files to solve the problem.

Further information on firmware updates can be found in the"UM EN MGUARD NT" user manual, available at phoenixcontact.net/product/1153079.

Application

– The device is to be updated to a higher firmware version from an SD card, without access to a management interface.

The device configuration, passwords and certificates are to remain unaltered.

Result

– The firmware of the device is updated to a higher version by means of the update file stored on the SD card.
– The device configuration, passwords and certificates remain unaltered.

Requirement

– A (single) valid update file signed by Phoenix Contact has to be stored on the first partition of the SD card.

Note: If there is a second update file stored on the SD card, the *Smart Mode* function will be aborted: the PF1–5 LEDs light up red.

– An "update" to the same or a downgrade to a lower firmware version is not possible and leads to an abortion of the process: the PF1–5 LEDs light up red.

Execution

⇒ see “Using „Smart mode“” on page 47

Updating from SD card
PF1
PF2
PF3
PF4
PF5

5.2 Using „Smart mode“

The *Smart Mode* can be activated by pressing the Mode button after the device has been started.

Only press the Mode button after you have started the device.
If the Mode button is already being pressed during the device start, it is subsequently not possible to access the device. In this case, restart the device by briefly interrupting the power supply.

5.2.1 Activating „Smart mode“

- Start the device by connecting it to the supply voltage.
- Press and hold the Mode button within two seconds.

⇒ After approx. 5 seconds, all PF LEDs (PF1–5) flash green.

- Release the Mode button.

⇒ The selected *Smart Mode* function is indicated by the corresponding PF LED (green) (see Table 5-1).

⇒ In addition, all PF LEDs flash green three times every four seconds.

⇒ After activation, the “Exit without changes” function is selected.

5.2.2 Selecting „Smart mode“ function

- Briefly press the Mode button to select the next function in each case.

⇒ The selected function is indicated by the respective PF LED (see below).

Table 5-1 *Smart Mode* functions in “Selected” status

Exiting without changes	Restoring configuration access	Restoring the factory settings	Updating from SD card
PF1	PF1	PF1	PF1
PF2	**PF2**	PF2	PF2
PF3	PF3	**PF3**	PF3
PF4	PF4	PF4	**PF4**
PF5	PF5	PF5	PF5
Additionally, PF1–5 flash green simultaneously three times every four seconds.			

5.2.3 Executing „Smart mode“ function

- To execute the selected function, proceed as follows:
  - Press and hold the Mode button.

  ⇒ After approx. 5 seconds, all PF LEDs flash green (fast).

  - Release the Mode button.

⇒ The selected function is executed.

⇒ All PF LEDs that are not assigned to the function light up orange (see Section 5.2.5).

- **NOTE: Do not interrupt the power supply to the device!**
  An interruption in the power supply can cause a device defect.

⇒ If all PF LEDs light up in green, the function has been executed successfully.

- Restart the device.

5.2.4 Exiting „Smart mode“

The only way to exit *Smart Mode* is by selecting and applying a *Smart Mode* function:

- *Smart Mode* function PF1: *Smart Mode* is exited without applying changes. The device restarts.
- *Smart Mode* functions PF2–4: The selected *Smart Mode* function is performed. After the *Smart Mode* function has been completed successfully, the device has to be re-started.

5.2.5 LED indicator (Smart mode)

Example “Restoring the factory settings”

Table 5-2 LED indicator: *Smart mode* “Restore factory settings”

Selected	Is being executed	Completed successfully	Failed
PF1 PF2 **PF3** PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5	PF1 PF2 PF3 PF4 PF5
The LED shows which *Smart mode* function has been selected (see Table 5-1). Additionally, PF1–5 flash green simultaneously three times every four seconds.	The *Smart mode* function is executed: The firmware is written to the device. **NOTE: An interruption in the power supply can damage the device!** **Do not switch off the device!** Wait until the function has been executed successfully.	The *Smart mode* function has been executed successfully. Restart the device.	In the event of an error, restart the device. If the error persists, contact your support. A severe error can also be indicated by the “FAIL” LED.

6 Device replacement, device defect, and repair

6.1 Secure deletion of sensitive data

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.
Execute the "Restoring the factory settings" *Smart Mode* to securely and irrevocably delete data on the device (see Section 5.1.3).

6.2 Device replacement

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

You can replace the device if necessary.

- Disconnect the device from the power supply.
- Remove all cables.
- Remove the SD card.
- Remove the device as described in Section 3.1.
- Replace the device with an identical device (the same Order No.), factory new or with factory settings (see Section 5.1).
- (Optional): Restore a saved configuration of the previous device on the new device (see Section 6.2.1).

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

A detailed description can be found in the "UM EN MGUARD NT" user manual, available at phoenixcontact.net/product/1153079).

The following applies to all **new devices** or devices that have been reset to factory settings using *Smart Mode* (see Section 5.1.3):

A configuration or user management saved on the inserted SD card is automatically imported into the device and applied there when the device is started or commissioned.

Prerequisite:

– The saved configuration is contained on the SD card: individually (*users_pass.json, snmp-pass.conf* and *configuration.json*) or in packed form (*mGuard.tar.gz*). The single files are used with priority!
– Firmware version "SD card" is lower/equal to firmware version "Device".
– If an error occurs during the import, the device starts in the factory settings. The FAIL and PF1 LEDs additionally light up red.

6.3 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 7).
  - 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.

6.4 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.

7 Technical data

7.1 FL MGUARD 1102/1105

Table 7-1 Technical data

General data (FL MGUARD 1102 / FL MGUARD 1105)	
Platform	Marvell Armada 3720
Network interfaces	
FL MGUARD 1102	2 Ethernet interfaces with: – RJ45 I full duplex I auto MDIX – Ethernet (10Base-T/IEEE 802.3i) – Fast Ethernet (100Base-TX/IEEE 802.3u) – Gigabit Ethernet (1000Base-T/IEEE 802.3ab)
FL MGUARD 1105	5 Ethernet interfaces with: – RJ45 I full duplex I 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 I digital I/Os I log files
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor
Ambient temperature (operation)	0°C ... +60 °C
Ambient temperature (storage/transport)	-40°C ... +70 °C
Permissible humidity (operation)	5 % ... 95 % (non-condensing)
Degree of protection	IP20
Protection class	Class 3 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
Overvoltage category	None
Mounting position	Perpendicular to a standard DIN rail
Connection to protective earth 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	270 g 297 g

Firmware and power values	
Supported firmware	mGuardNT 1.3.2 or later
Management support	Web-based management I RESTful Configuration API I SD card

Supply voltage (US1)

Connection	Via COMBICON connector (Push-in spring connection); maximum conductor cross section = 1.5 mm² (use copper wires that are suitable for *90 °C* or equivalent)
Nominal value	24 V DC
Permissible voltage range	
FL MGUARD 1102 FL MGUARD 1105	18 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)	
FL MGUARD 1102	1.00 A
FL MGUARD 1105	1.06 A
Typical current consumption (US = 24 V, T_{amb} = 20 °C, DO_I = 0 A)	
FL MGUARD 1102	0.12 A
FL MGUARD 1105	0.18 A
Test voltage	500 V DC for one minute

Network interfaces

Properties of RJ45 connections	
Number	
FL MGUARD 1102	2
FL MGUARD 1105	5
Connection format	8-pos. RJ45 jack
Connection medium	Twisted-pair cable with a conductor cross section of 0.14 mm² to 0.22 mm²
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	18 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

Other

Conformance	CE conformity

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**

108413_en_11
Order No. —11

INSPIRING INNOVATIONS