Installing and starting up the mGuard hardware

User manual

PHOENIX CONTACT
INSPIRING INNOVATIONS

User manual

Installing and starting up the mGuard hardware

2022-11-08

Designation: UM EN MGUARD DEVICES

Revision: 09

Order No.: —

This user manual is valid for the following devices of the mGuard product range:

- FL MGUARD RS4000
- FL MGUARD RS2000
- FL MGUARD RS4004
- FL MGUARD RS2005
- TC MGUARD RS4000 3G
- TC MGUARD RS2000 3G
- TC MGUARD RS4000 4G (incl. US versions VZW and ATT)
- TC MGUARD RS2000 4G (incl. US versions VZW and ATT)
- FL MGUARD RS2000 TX/TX-B
- FL MGUARD RS4000 TX/TX-P
- FL MGUARD RS4000 TX/TX VPN-M
- FL MGUARD GT/GT
- FL MGUARD SMART2
- FL MGUARD PCI(E)4000
- FL MGUARD CENTERPORT
- FL MGUARD DELTA TX/TX

Please observe the following notes

User group of this manual

The use of products described in this manual is oriented exclusively to qualified electricians or persons instructed by them, who are familiar with applicable standards and other regulations regarding electrical engineering and, in particular, the relevant safety concepts.

Explanation of symbols used and signal words

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety measures that follow this symbol to avoid possible injury or death.

There are three different categories of personal injury that are indicated with a signal word.

DANGER This indicates a hazardous situation which, if not avoided, will result in death or serious injury.

WARNING This indicates a hazardous situation which, if not avoided, could result in death or serious injury.

CAUTION This indicates a hazardous situation which, if not avoided, could result in minor or moderate injury.

This symbol together with the signal word **NOTE** and the accompanying text alert the reader to a situation which may cause damage or malfunction to the device, hardware/software, or surrounding property.

This symbol and the accompanying text provide the reader with additional information or refer to detailed sources of information.

How to contact us

Internet

Up-to-date information on <Variable>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

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

General terms and conditions of use for technical documentation

<Variable>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 <Variable>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 <Variable>Phoenix Contact apply exclusively, in particular as concerns any warranty liability.

FCC Note

The FCC Statement applies to the following devices:

Class A: FL MGUARD RS4000, FL MGUARD RS2000, FL MGUARD RS4004, FL MGUARD RS2005, FL MGUARD SMART2, FL MGUARD PCI4000, FL MGUARD DELTA TX/TX, FL MGUARD GT/GT, FL MGUARD RS2000 TX/TX-B, FL MGUARD RS4000 TX/TX-P, FL MGUARD RS2000 TX/TX VPN-M.

Class B: TC MGUARD RS4000 3G, TC MGUARD RS2000 3G, FL MGUARD RS4000 4G, FL MGUARD RS2000 4G, FL MGUARD CENTERPORT.

FCC Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

FCC Statement

Class A	Class B
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.	This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures: – Reorient or relocate the receiving antenna. – Increase the separation between the equipment and receiver. – Connect the equipment into an outlet on a circuit different from that to which the receiver is connected. – Consult the dealer or an experienced radio/TV technician for help. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. **FCC RF radiation Exposure Statement:** This equipment complies with FCC RF exposure limits set forth for an uncontrolled environment. The antenna(s) used for this transmitter must be installed and operated with a minimum separation distance of 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter expect in accordance with the FCC multi-transmitter policy.

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 optional IPsec and OpenVPN. They are suitable for distributed protection of production cells or individual machines against manipulation and for secure remote maintenance. The devices have been designed to accommodate strict distributed security and high availability requirements.

1.5 Modifications to the product

The device must not be opened or modified. Do not repair the device yourself, replace it with an equivalent device. Repairs may only be carried out by the manufacturer. The manufacturer is not liable for damage resulting from violation.

1.6 Safety notes

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

DIN rail devices are 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.
- The IP20 degree of protection (IEC/EN 60529-0/EN 60529-0) specifies that the device is intended for use in a clean and dry environment. Do not subject the device to mechanical and/or thermal stress that exceeds the specified limits.
- To avoid overheating, do not expose the device to direct sunlight or other heat sources.

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).
- Clean the device housing with a soft cloth. Do not use aggressive solvents.

1.6.1 UL/HazLoc information

– This equipment is an open-type device meant to be installed in an enclosure suitable for the environment that is only accessible with the use of a tool.
– Suitable for use in class I, division 2, groups A, B, C and D hazardous locations, or non-hazardous locations only.
– WARNING - Explosion Hazard - Substitution of any components may impair suitability for Class I, Division 2.
– WARNING - Explosion Hazard - Do not disconnect equipment while the circuit is live or unless the area is known to be free of ignitable concentrations.
– AVERTISSEMENT - Risque d'explosion - Tout remplacement d'un composant peut entraver la fiabilité pour Classe I, Division 2. components may impair suitability for Class I, Division 2.
– AVERTISSEMENT - Risque d'explosion - Ne pas déconnecter l'équipement lorsque le circuit est sous tension ou sauf si la zone est connue pour être exempte de concentrations inflammables.

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 2022-09-13; 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/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 (UM EN MGUARD). Available in the download area of the corresponding product page in the Phoenix Contact Web Shop, e. g. phoenixcontact.net/products or help.mguard.com

2 FL MGUARD RS4000/RS2000

Table 2-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD RS4000 TX/TX	2700634
FL MGUARD RS4000 TX/TX VPN	2200515
FL MGUARD RS2000 TX/TX VPN	2700642

Product description

The **FL MGUARD RS4000** is a security router with intelligent firewall and optional IPsec VPN (optionally up to 10 or up to 250 tunnels). It has been designed for use in industry to accommodate strict distributed security and high availability requirements.

The **FL MGUARD RS2000** is a version with basic firewall and integrated IPsec VPN (maximum of two tunnels). Its scope of functions is reduced to the essentials. It is suitable for secure remote maintenance applications in industry and enables the quick startup of robust field devices for industrial use, thereby facilitating error-free, independent operation.

Both versions support a replaceable configuration memory in the form of an SD card. (The SD cards are not supplied as standard.) The fanless metal housing is mounted on a DIN rail.

The following connectivity options are available

FL MGUARD RS4000: (LAN/WAN)		FL MGUARD RS2000: (LAN/WAN)	
TX/TX	Ethernet/Ethernet	TX/TX VPN	Ethernet/Ethernet + VPN
TX/TX VPN	Ethernet/Ethernet + VPN		

Figure 2-1 FL MGUARD RS4000/RS2000

2.1 Operating elements and LEDs

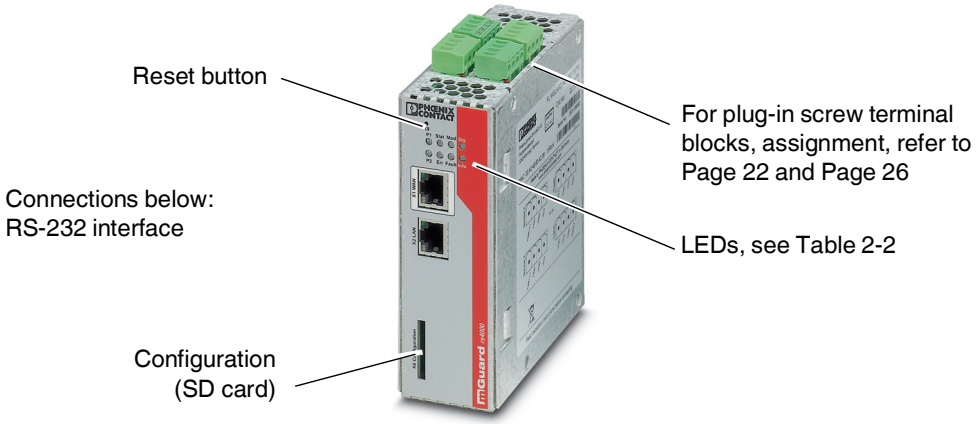


Figure 2-2 Operating elements and LEDs on the FL MGUARD RS4000

Table 2-2 LEDs on the FL MGUARD RS4000 and FL MGUARD RS2000

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active (FL MGUARD RS2000: not used)
STAT	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
ERR	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see Page 35) or contact your dealer.
STAT+ ERR	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
SIG	–		(Not used)
FAULT	Red	On	The signal output changes to the low level due to an error (inverted control logic) (see Page 24 or Page 25). The signal output is inactive during a restart.
MOD	Green	On	Connection via modem established

Table 2-2 LEDs on the FL MGUARD RS4000 and FL MGUARD RS2000 [...]

LED	State		Meaning
INFO	Green	On	Up to firmware version 8.0: the configured VPN connection has been established As of firmware version 8.1, the configured VPN connections are established or the firewall rule records defined at output O1 are activated
		Flashing	Up to firmware version 8.0: the configured VPN connection is being established or aborted As of firmware version 8.1: the configured VPN connections are being established or aborted or the defined firewall rule records are activated or deactivated.
LAN	Green	On	The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED)
WAN	Green	On	**Ethernet status.** Indicates the status of the LAN or WAN port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN or WAN. When data packets are transmitted, the LED goes out briefly.

2.2 Startup

2.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  -20°C ... +60°C
– Maximum humidity, non-condensing
  5% ... 95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

2.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– The device
– Package slip
– Plug-in screw terminal blocks for the power supply connection and inputs/outputs (inserted)

2.3 Installation of FL MGUARD RS4000/RS2000

2.3.1 Mounting/removal

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Mount the FL MGUARD RS4000/RS2000 on a grounded 35 mm DIN rail according to DIN EN 60715.

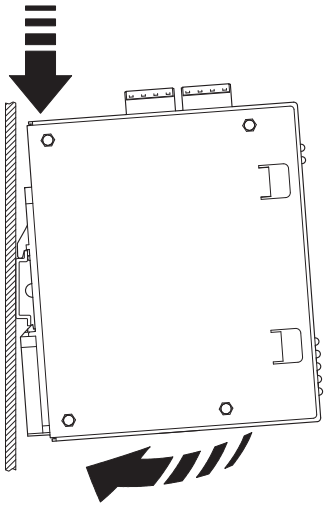


Figure 2-3 Mounting the FL MGUARD RS4000/RS2000 on a DIN rail

- Attach the top snap-on foot of the FL MGUARD RS4000/RS2000 to the DIN rail and then press the FL MGUARD RS4000/RS2000 down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the FL MGUARD RS4000/RS2000 from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the FL MGUARD RS4000/RS2000.

2.3.2 Connecting to the network

NOTE: Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

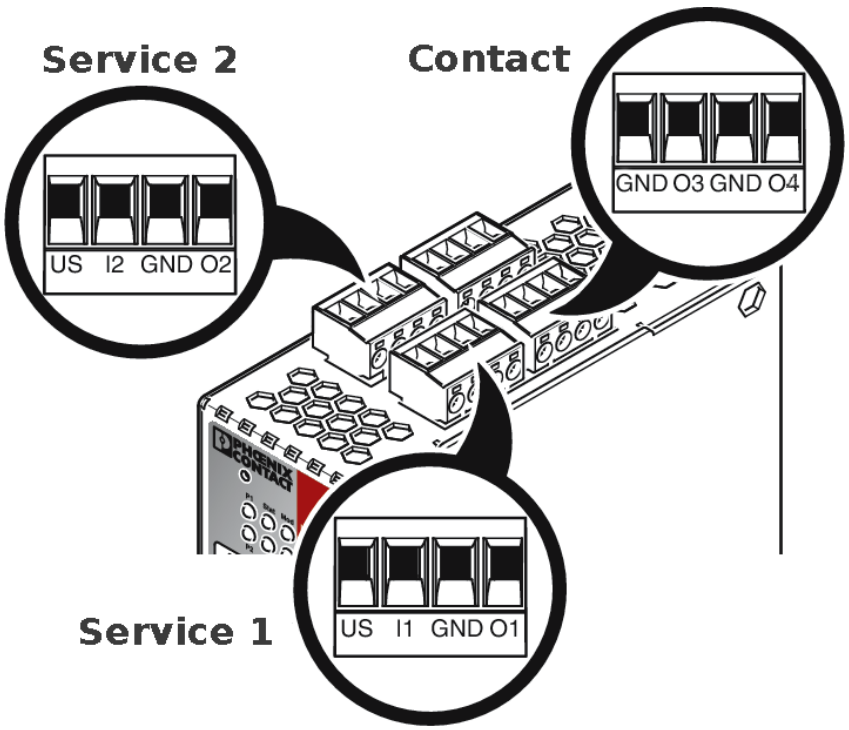
- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply.
- Connect the internal network interface LAN 1 of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

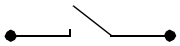
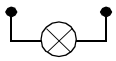
2.3.3 Service contacts

NOTE: Do **not** connect the voltage and ground outputs **US** (resp. **CMD V+**) and **GND** to an external voltage source.

Please note that only the “Service 1” contacts are used with firmware version up to and including 7.6.x. The “Service 2” contacts shall be made available as of firmware version 8.1.

The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.



Service 1 + 2	US	I1/I2	GND	O1/O2
	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output [1]
	Example 		Example 	

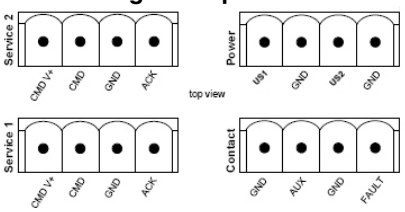
Power	24V	0V	24V	0V
	+24 V	0 V	+24 V	0 V
	See Section 2.3.4		Only for FL MGUARD RS4000 See Section 2.3.4	

Contact	GND	O3	GND	O4
	Not used	Not used	Signal output (-)	Signal output (+)[2]

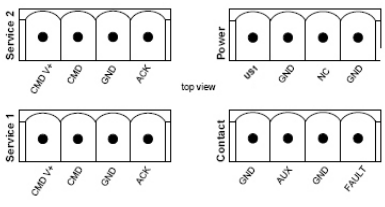
[1] Maximum of 250 mA at 11 ... 36 V DC

[2] 11 V ... 36 V when operating correctly; disconnected in the event of a fault

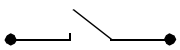
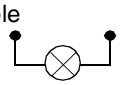
The following description of the contacts is also possible:



FL MGUARD RS4000



FL MGUARD RS2000

Service 1 + 2	CMD V+	CMD	GND	ACK
	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output [1]
	Example 		Example 	

Power	US1	GND	US2	GND
	+24 V	0 V	+24 V	0 V
	See Section 2.3.4		Only for FL MGUARD RS4000 See Section 2.3.4	

Contact	GND	AUX	GND	FAULT
	Not used	Not used	Signal output (-)	Signal output (+)[2]

[1] Maximum of 250 mA at 11 ... 36 V DC

[2] 11 V ... 36 V when operating correctly; disconnected in the event of a fault

A **push button** or an **on/off switch** (e.g., key switch) can be connected between **service contacts US** and **I** (resp. CMD V+ and CMD).

The **contacts O1/O2 (+)** and **O4 (+)** (resp. ACK and FAULT) are non-floating, continuously short-circuit-proof and supply a maximum of 250 mA.

The switching inputs and switching outputs can be connected with signals from external devices, e.g., with signals from PLCs. In this case, ensure the same potential as well as voltage and current specifications are defined.

Depending on the firmware version used, the service contacts can be used for various switching or signaling tasks.

Service contacts as of firmware version 8.1

Input/CMD I1, CMD I2

Via the web interface under “Management, Service I/O”, you can set whether a push button or an on/off switch has been connected to the inputs. One or more freely selectable VPN connections or firewall rule records can be switched via the corresponding switch. A mixture of VPN connections and firewall rule records is also possible. The web interface displays which VPN connections and which firewall rule records are connected to this input.

The push button or on/off switch is used to establish and release predefined VPN connections or the defined firewall rule records.

Operating a connected push button

- To switch on the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.
- To switch off the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.

Operating a connected on/off switch

- To switch on the selected VPN connections or firewall rule records, set the switch to ON.
- To switch off the selected VPN connections or firewall rule records, set the switch to OFF.

Signal contact (signal output) O1, O2 resp. ACK

Via the web interface under “Management, Service I/O” you can set whether certain VPN connections or firewall rule records are monitored and displayed via the LED Info 1 (output/O1 resp. ACK) or LED Info 2 (output/O2 resp. ACK).

If VPN connections are being monitored, an illuminated Info LED indicates that VPN connections are established.

Alarm output O4 resp. FAULT

The O4 alarm output monitors the function of the FL MGUARD RS4000/RS2000 and therefore enables remote diagnostics.

The Fault LED lights up red if the signal output changes to the low level due to an error (inverted control logic).

The O4 alarm output reports the following when “Management, Service I/O, Alarm output” has been activated.

– Failure of the redundant supply voltage
– Monitoring of the link status of the Ethernet connections
– Monitoring of the temperature condition
– Monitoring of the redundancy status
– Monitoring of the connection state of the internal modem

Service contacts up to firmware version 8.0

The push button or on/off switch is used to establish and release a predefined VPN connection.

The output indicates the status of the VPN connection (in the web interface under “IPsec VPN >> Global >> Options”).

Operating a connected push button

- To establish the VPN connection, hold down the button for a few seconds until the INFO LED flashes. Only then release the button.

  Flashing indicates that the device has received the command to establish the VPN connection and is establishing the VPN connection. As soon as the VPN connection is established, the INFO LED remains lit continuously.
- To release the VPN connection, hold down the button for a few seconds until the signal output flashes or goes out. Only then release the button.

  As soon as the INFO LED goes out, the VPN connection is released.

Operating a connected on/off switch

- To establish the VPN connection, set the switch to the ON position.
- To release the VPN connection, set the switch to the OFF position.

INFO LED

If the INFO LED does not light up, this generally indicates that the defined VPN connection is not present. Either the VPN connection was not established or it has failed due to an error.

If the INFO LED is illuminated, the VPN connection is present.

If the INFO LED is flashing, the VPN connection is being established or released.

Signal contact (signal output)

The signal contact monitors the function of the FL MGUARD RS4000/RS2000 and thus enables remote diagnostics.

The FAULT LED lights up red if the signal output changes to the low level due to an error (inverted control logic).

The voltage at the signal contact corresponds to the supply voltage applied. The following is reported when monitoring the output voltage:

– Failure of at least one of the two supply voltages.
– Power supply of the FL MGUARD RS4000/RS2000 below the limit value (supply voltage 1 and/or 2 lower than 11 V).
– Link status monitoring of the Ethernet connections, if configured. By default upon delivery, the connection is not monitored. Monitoring can be activated (on the web interface under “Management >> System Settings >> Signal Contact”).
– Error during selftest.

During a restart, the signal contact is switched off until the FL MGUARD RS4000/RS2000 has started up completely. This also applies when the signal contact is manually set to “Closed” under “Manual settings” in the software configuration.

2.3.4 Connecting the supply voltage

WARNING: The FL MGUARD RS4000/RS2000 is designed for operation with a DC voltage of 11 V DC ... 36 V DC/SELV, 1.5 A, maximum.

Therefore, only SELV circuits with voltage limitations according to EN 60950-1 may be connected to the supply connections and the signal contact.

The supply voltage is connected via a plug-in screw terminal block, which is located on the top of the device.

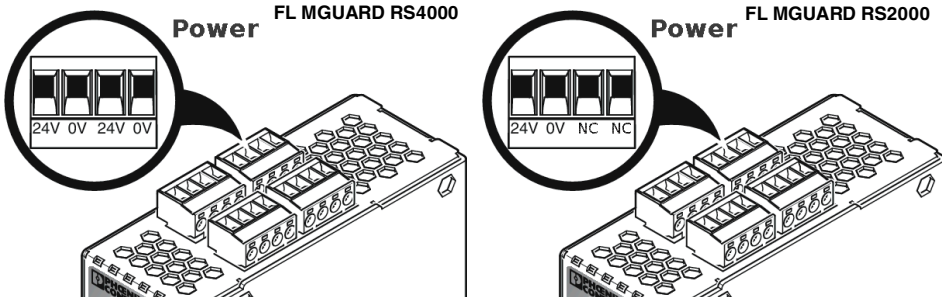


Figure 2-4 Connecting the supply voltage

Instead of the designation **24V/24V** the designation **US1/US2** is also used.

The **FL MGUARD RS4000** has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Do not connect the service contacts to an external voltage source.
- Wire the supply voltage lines with the corresponding screw terminal block **24V/24V** (resp. US1/US2) of the device. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the screw terminal blocks into the intended sockets on the top of the device (see Figure 2-4).

Status LED P1 lights up green when the supply voltage has been connected properly. On the FL MGUARD RS4000, the status indicator P2 also lights up if there is a redundant supply voltage connection.

The device boots the firmware. Status STAT LED flashes green. The device is ready for operation as soon as the Ethernet socket LEDs light up. Additionally, status LEDs P1/P2 light up green and the status STAT LED flashes green at heartbeat.

Redundant voltage supply (FL MGUARD RS4000)

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the FL MGUARD RS4000 alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the FL MGUARD RS4000 indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs **24V/24V** (resp. US1/US2)) or by installing an appropriate wire jumper between connections **24V and 24V** (resp. US1 and US2).

2.4 Preparing the configuration

2.4.1 Connection requirements

- The **FL MGUARD RS4000/RS2000** must be connected to at least one active power supply unit.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
- **For remote configuration**: The device must be configured so that remote configuration is permitted.
- The device must be connected, i.e., the required connections must be working.

2.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following addresses:

Table 2-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 31). Alternatively, you can select a different stealth configuration or use another network mode.

2.5 Configuration in Stealth mode

On initial startup, the device can be accessed via two addresses:

– https://192.168.1.1/ (see Page 29)
– https://1.1.1.1/ (see Page 29)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 30).

The device can be accessed via https://192.168.1.1/ if the external network interface is not connected on startup.

Computers can access the device via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the device. For this purpose, the device with LAN port and WAN port must be integrated in an operational network in which the default gateway can be accessed via the WAN port.

– After access via IP address 192.168.1.1 and successful login, IP address 192.168.1.1 is set as a fixed management IP address.
– After access via IP address 1.1.1.1 or after IP address assignment via BootP, the product can no longer be accessed via IP address 192.168.1.1.

2.5.1 IP address 192.168.1.1

In Stealth mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.

– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

2.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the device to be addressed via address **https://1.1.1.1/,** it must be connected to a configured network interface. This is the case if it is connected in an existing network connection and if the default gateway can be accessed via the WAN port of the device at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 31). Continue from this point.

After access via IP address 1.1.1.1, the product can no longer be accessed via IP address 192.168.1.1

2.5.3 Assigning the IP address via BootP

After assigning an IP address via BootP, the product can no longer be accessed via IP address 192.168.1.1

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

Section 14.1 explains IP address assignment using the free Windows software "IP Assignment Tool" (IPAssign.exe).

Notes for BootP

During initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the device no longer sends BootP requests. The product 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) must be performed.

2.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via one of the following addresses:

Table 2-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 2-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 35).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 27).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.

  Click on “Properties” under “LAN settings”.

  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 2-5 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

2.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

2.8 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (Default)

2.9 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

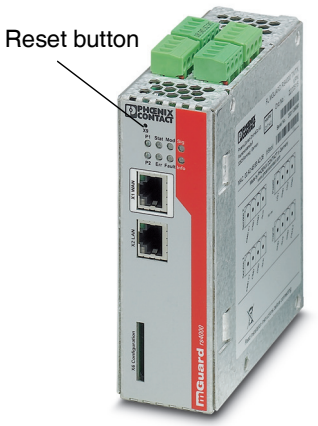


Figure 2-6 Reset button

2.9.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the ERR LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

2.9.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

When performing the recovery procedure, the default network settings are established:

Table 2-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is reset to Stealth mode with the default setting “multiple Clients”.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The configured IP address of the device differs from the default setting.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 2-6 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately 2 seconds, the STAT LED lights up green.
- Press the Reset button slowly again six times.
  If successful, the STAT LED lights up green.
  If unsuccessful, the ERR LED lights up red.

If successful, the device restarts after two seconds and switches to Stealth mode. The device can then be reached again under the corresponding addresses.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

2.9.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

- **All configured settings are deleted.** The device is set to the delivery state.
- In mGuard firmware version 5.0.0 or later, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

- All necessary firmware files must be located in a common directory on the first partition of the SD card
- This partition must use a VFAT file system (standard type for SD cards).

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

- The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.
- This SD card has been inserted into the device.
- The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s

  Firmware/ubifs.img.mpc83xx.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the STAT, MOD, and SIG LEDs light up green. Then, the device is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**
  If the Reset button is not released, the device is restarted.
  The device now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.
  The STAT LED flashes.
  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.
  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.
  The STAT, MOD, and SIG LEDs form a running light.
  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.
  This process takes around 3 to 5 minutes. The STAT LED is lit continuously.
  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the STAT, MOD, and SIG LEDs flash green simultaneously.

- Restart the device. To do this, briefly press the Reset button.
  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 31).

2.10 Technical data

Hardware properties	FL MGUARD RS4000	FL MGUARD RS2000
Platform	Freescale network processor with 330 MHz clocking	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 I full duplex I auto MDIX	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232 I D-SUB 9 connector 2 digital inputs and 2 digital outputs	Serial RS-232 I D-SUB 9 connector 2 digital inputs and 2 digital outputs
Memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory
Redundancy options	Optional: VPN I router and firewall	Not available
Power supply	Voltage range 11 ... 36 V DC, redundant	Voltage range 11 ... 36 V DC
Power consumption	2.13 W, typical	2.13 W, typical
Humidity range	5% ... 95% (operation, storage), non-condensing	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20	IP20
Temperature range	-20°C ... +60°C (operation) -20°C ... +60°C (storage)	-20°C ... +60°C (operation) -20°C ... +60°C (storage)
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)	130 x 45 x 114 mm (up to DIN rail support)
Weight	725 g (TX/TX)	725 g (TX/TX)
Weight (incl. packaging)	900 g (TX/TX)	900 g (TX/TX)

Firmware and power values	FL MGUARD RS4000	FL MGUARD RS2000
Firmware compatibility	For mGuard v7.4.0 or later: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.	
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: 120 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum.	
Virtual Private Network (VPN)	IPsec (IETF standard) Optionally up to 250 VPN tunnels	IPsec (IETF standard) Up to 2 VPN tunnels
Hardware-based encryption	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: 30 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 20 Mbps, maximum	
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software	
Diagnostics	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) signal contacts I service contacts I log file I remote syslog	LEDs (Power, State, Error, Signal, Fault, Modem, Info) signal contacts I service contacts I log file I remote syslog

Other	FL MGUARD RS4000	FL MGUARD RS2000
Conformance	CE I FCC I UL 508 ANSI/ISA 12.12 Class I Div. 2	
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Remote Services Portal ready	

3 FL MGUARD RS4004/RS2005

Table 3-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD RS4004 DTX/TX	2701876
FL MGUARD RS4004 TX/TX VPN	2701877
FL MGUARD RS2005 TX VPN	2701875

Product description

The **FL MGUARD RS4004** is suitable for distributed protection of production cells or individual machines against manipulation.

It features a 4-port managed LAN switch, one WAN port and one DMZ port, and a serial interface.

The serial interface can be switched to the WAN interface as redundancy path, for example. A dedicated DMZ port with its own firewall rules enables segmentation and differentiated security concepts. You can integrate automation devices with serial interfaces into networks, as a COM server is integrated.

For software-independent remote maintenance, the FL MGUARD RS4004 can be used as a VPN router for optionally up to 250 parallel, IPsec-encrypted VPN tunnels.

The **FL MGUARD RS2005** is a version with basic firewall and can be used as a VPN client for up to two parallel, IPsec-encrypted VPN tunnels. It is suitable for secure remote maintenance applications and enables connection of globally distributed machines and controllers.

Both versions support a replaceable configuration memory in the form of an SD card. To increase security, VPN connections can be switched on or off via a switch contact or software interface. The fanless metal housing is mounted on a DIN rail.

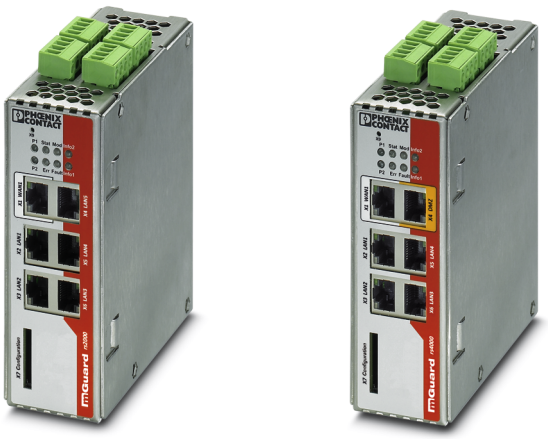


Figure 3-1 FL MGUARD RS2005/FL MGUARD RS4004

3.1 Operating elements and LEDs

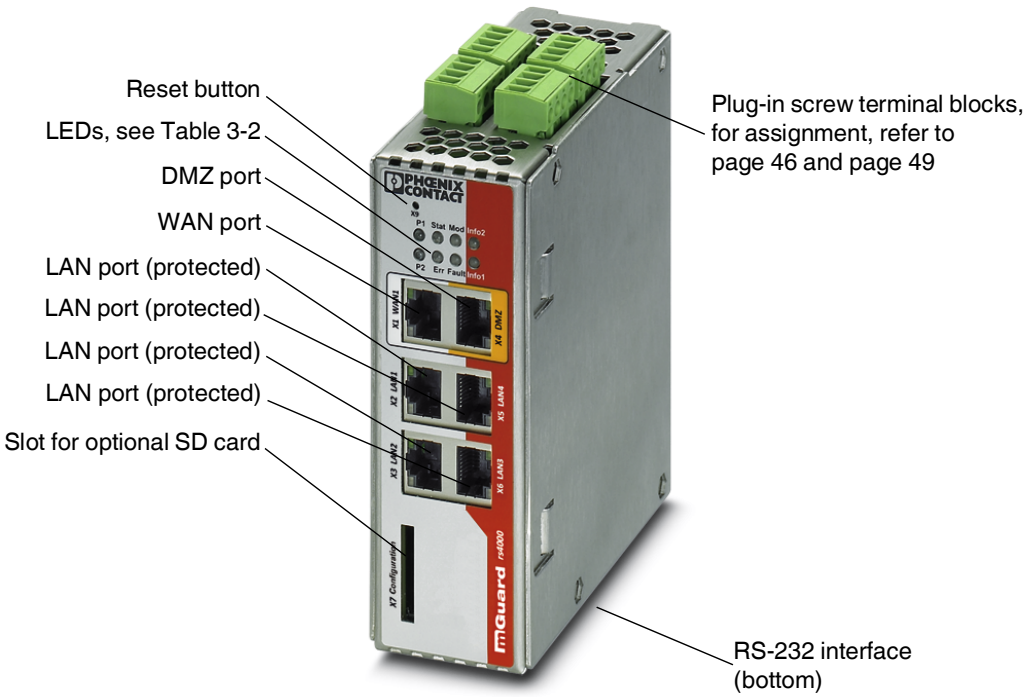


Figure 3-2 Operating elements and LEDs on the FL MGUARD RS4004

Table 3-2 LEDs on the FL MGUARD RS4004 and FL MGUARD RS2005

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active (FL MGUARD RS2005: not used)
Stat	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
Err	Red	Flashing	**System error**. Restart the device. – Press the reset button shortly (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see page 55) or contact your dealer.
Stat + Err	Flashing alternately: green and red		**Boot process**. When the device has been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
Mod	Green	On	Connection via modem established
Fault	Red	On	The signal output changes to the low level due to an error (inverted control logic). The signal output is inactive during a restart.

Table 3-2 LEDs on the FL MGUARD RS4004 and FL MGUARD RS2005 [...]

LED	State		Meaning
Info2	Green	On	The configured VPN connections are established at output O1 or the firewall records defined at output O1 are activated.
		Flashing	The configured VPN connections are being established or aborted at output O1 or the firewall rule records defined at output O1 are activated or deactivated.
Info1	Green	On	The configured VPN connections are established at output O2 or the firewall records defined at output O2 are activated.
		Flashing	The configured VPN connections are being established or aborted at output O2 or the firewall rule records defined at output O2 are activated or deactivated.
WAN 1	Green	On	The LEDs are located in the sockets (10/100 and duplex LED)
DMZ1[1]	Green	On	**Ethernet status**. The LEDs indicate the status of the relevant port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN, WAN or DMZ. When data packets are transmitted, the LED goes out briefly.
LAN 1–4/5[2]	Green	On	

[1] FL MGUARD RS4004 only

[2] FL MGUARD RS2005 only

3.2 Startup

3.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

For connecting a modem or serial terminal to the RS-232 interface, you will need a null modem cable not exceeding 10 m in length.

NOTE: Risk of damage to equipment due to noise emissions

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.

NOTE: Electrostatic discharge

When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and IEC 61340-5-1.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  -20°C ... +60°C
– Maximum humidity, non-condensing:
  5% ... 95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

3.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– Device
– Package slip
– Plug-in screw terminal blocks for the power supply connection and inputs/outputs (inserted)

3.2.3 mGuard-Firmware

The device must be operated with mGuard firmware version 8.1.5 or higher.

3.3 Installing the FL MGUARD RS4004/RS2005

3.3.1 Mounting/removal

NOTE: Device damage
Only mount and remove devices when the power supply is disconnected.

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Mount the FL MGUARD RS4004/RS2005 on a grounded 35 mm DIN rail according to DIN EN 60715.

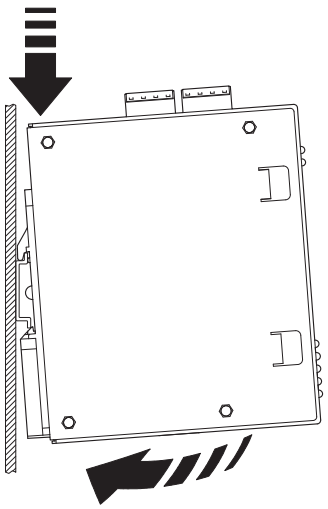


Figure 3-3 Mounting the FL MGUARD RS4004/RS2005 on a DIN rail

- Attach the top snap-on foot of the FL MGUARD RS4004/RS2005 to the DIN rail and then press the FL MGUARD RS4004/RS2005 down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the FL MGUARD RS4004/RS2005 from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the FL MGUARD RS4004/RS2005.

3.3.2 Connecting to the network

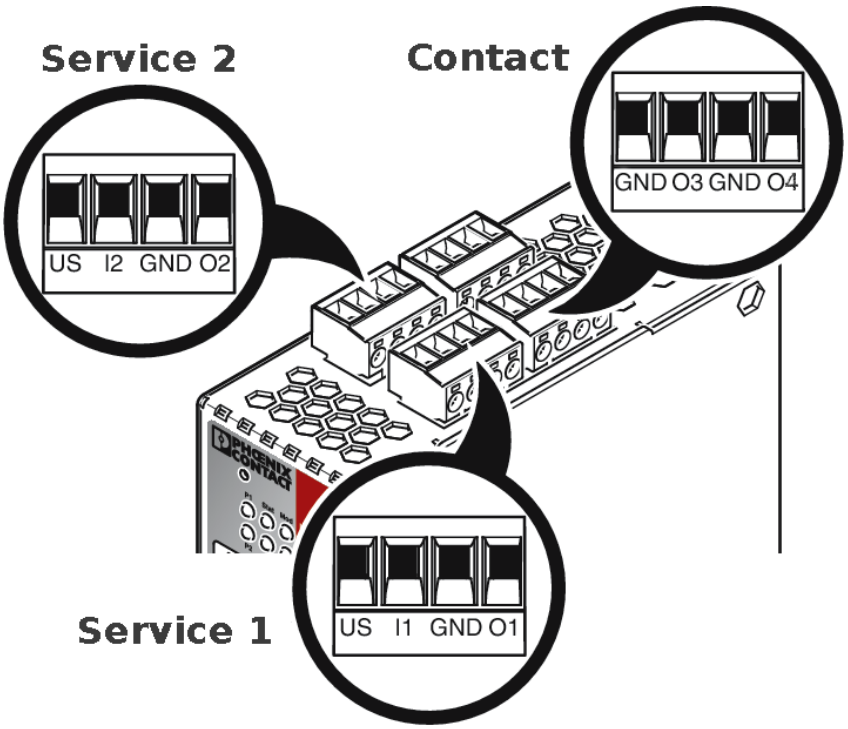
NOTE: Risk of material damage due to incorrect wiring
Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

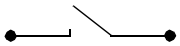
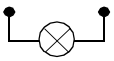
- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply.
- Connect the internal network interface LAN of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

3.3.3 Connecting the service contacts

NOTE: Do **not** connect the voltage and ground outputs **US** (resp. **CMD V+**) and **GND** to an external voltage source.

The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.



	US	I1/I2	GND	O1/O2
Service 1 + 2	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output [1]
	Example 		Example 	

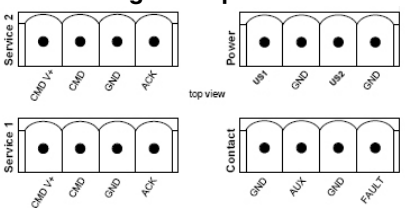
	24V	0V	24V	0V
Power	+24 V	0 V	+24 V	0 V
	See Section 3.3.4		Only for FL MGUARD RS4000 See Section 3.3.4	

	GND	O3	GND	O4
Contact	Not used	Not used	Signal output (-)	Signal output (+)[2]

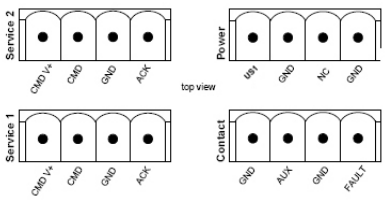
[1] Maximum of 250 mA at 11 ... 36 V DC

[2] 11 V ... 36 V when operating correctly; disconnected in the event of a fault

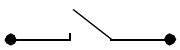
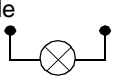
The following description of the contacts is also possible:



FL MGUARD RS4004



FL MGUARD RS2005

	CMD V+	CMD	GND	ACK
Service 1 + 2	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output [1]
	Example 		Example 	

	US1	GND	US2	GND
Power	+24 V	0 V	+24 V	0 V
	See Section 3.3.4		Only for FL MGUARD RS4004 See Section 3.3.4	

	GND	AUX	GND	FAULT
Contact	Not used	Not used	Signal output (-)	Signal output (+)[2]

[1] Maximum of 250 mA at 11 ... 36 V DC

[2] 11 V ... 36 V when operating correctly; disconnected in the event of a fault

A **push button** or an **on/off switch** (e.g., key switch) can be connected between **service contacts US** and **I** (resp. CMD V+ and CMD).

The **contacts O1/O2 (+)** and **O4 (+)** (resp. ACK and FAULT) are non-floating, continuously short-circuit-proof and supply a maximum of 250 mA.

The switching inputs and switching outputs can be connected with signals from external devices, e.g., with signals from PLCs. In this case, ensure the same potential as well as voltage and current specifications are defined.

Depending on the firmware version used, the service contacts can be used for various switching or signaling tasks.

3.3.4 Connecting the supply voltage

WARNING: The FL MGUARD RS4000/RS2000 is designed for operation with a DC voltage of 11 V DC ... 36 V DC/SELV, 1.5 A, maximum.

Therefore, only SELV circuits with voltage limitations according to EN 60950-1 may be connected to the supply connections and the signal contact.

The supply voltage is connected via a plug-in screw terminal block, which is located on the top of the device.

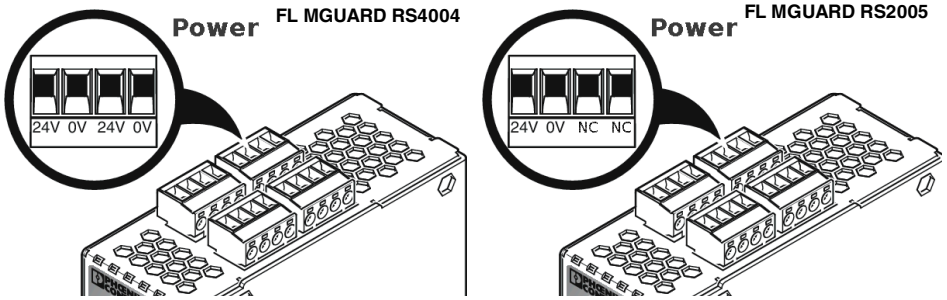


Figure 3-4 Connecting the supply voltage

Instead of the designation **24V/24V** the designation **US1/US2** is also used.

The **FL MGUARD RS4004** has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Do not connect the service contacts to an external voltage source.
- Wire the supply voltage lines with the corresponding screw terminal block **24V/24V** (resp. US1/US2) of the device. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the screw terminal blocks into the intended sockets on the top of the device (see Figure 3-4).

Status LED P1 lights up green when the supply voltage has been connected properly. On the FL MGUARD RS4004, the status indicator P2 also lights up if there is a redundant supply voltage connection.

The device boots the firmware. Status STAT LED flashes green. The device is ready for operation as soon as the Ethernet socket LEDs light up. Additionally, status LEDs P1/P2 light up green and the status STAT LED flashes green at heartbeat.

Redundant voltage supply (FL MGUARD RS4004)

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the FL MGUARD RS4004 alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the FL MGUARD RS4004 indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs **24V/24V** (resp. US1/US2)) or by installing an appropriate wire jumper between connections **24V and 24V** (resp. US1 and US2).

3.4 Preparing the configuration

3.4.1 Connection requirements

– The **FL MGUARD RS4004/RS2005** must be connected to at least one active power supply unit.
– **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
– **For remote configuration**: The device must be configured so that remote configuration is permitted.
– The device must be connected, i.e., the required connections must be working.

3.5 Configuration in Router mode

On initial startup, the device can be accessed via the following address:
– https://192.168.1.1

3.5.1 IP address 192.168.1.1

In Router mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.
– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:
- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

–

3.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via the following address:

Table 3-3 Preset address

Default setting	Network mode	Management IP #1 (IP address of the internal interface)
FL MGUARD RS2005	Router	https://192.168.1.1/
FL MGUARD RS4004	Router	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 3-3).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 55).

If the administrator web page is not displayed

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

- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.
  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.
  Click on “Properties” under “LAN settings”.
  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.
  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

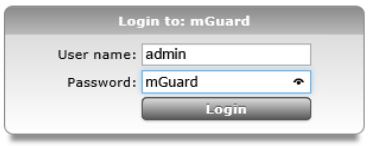


Figure 3-5 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

3.7 Remote configuration

Requirement

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

By default upon delivery, the option for remote configuration is disabled.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to software reference manual.

3.8 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

3.9 Restart, recovery procedure, and flashing the firmware

The reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

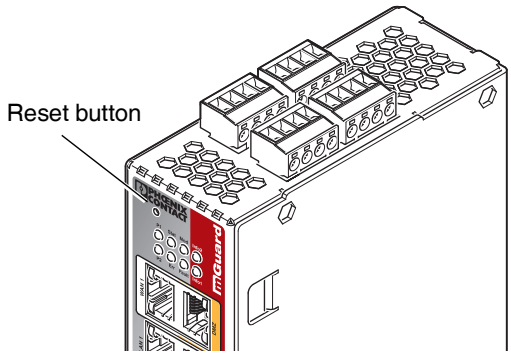


Figure 3-6 Reset button

3.9.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the reset button for around 1.5 seconds until the Err LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

3.9.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

Use the recovery procedure in case you have forgotten the IP address under which the device can be accessed.

The following network setting is restored:

Table 3-4 Restored network setting

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

The device is reset to router mode with the fixed IP address.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU configuration is activated for the Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The IP address of the device has been configured and is not known.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 3-5 Restored network setting

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the reset button six times.
  After approximately two seconds, the Stat LED lights up green.
- When the Stat LED has gone out, slowly press the reset button again six times.
  If successful, the Stat LED lights up green.
  If unsuccessful, the Err LED lights up red.

If successful, the device restarts after two seconds and switches to Router mode. The device can then be reached again under the corresponding address.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

3.9.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire firmware of the device should be reloaded on the device.

– **All configured settings are deleted.** The device is set to the delivery state.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

– All necessary firmware files must be located in a common directory on the first partition of the SD card

– This partition must use a VFAT file system (standard type for SD cards)

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

– The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.

– This SD card has been inserted into the device.

– The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s

  Firmware/ubifs.img.mpc83xx.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the reset button until the Stat, Mod, and Sig LEDs light up green. The device then is in rescue status.
- **Release the reset button within one second of entering rescue status.**

  If the reset button is not released, the device is restarted.

  The device now starts the rescue system: It first searches for an inserted SD card and for the relevant firmware there. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The Stat LED flashes.

  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.

  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.

  The Stat, Mod, and Sig LEDs form a running light.

  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual operating system and is signed electronically. Only files signed by the manufacturer are accepted.

  This process takes around 3 to 5 minutes. The Stat LED is lit continuously.

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the Stat, Mod, and Sig LEDs flash green simultaneously.

- Restart the device. To do so, press the reset button.

  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 51).

3.10 Technical data

Hardware properties	FL MGUARD RS4004	FL MGUARD RS2005
Platform	Freescale network processor	Freescale network processor
Network interfaces	4 LAN ports (managed)	1 DMZ port	1 WAN port Ethernet IEEE 802.3 10/100 Base TX RJ45	full duplex	auto MDIX	5 LAN ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ45	full duplex	auto MDIX
Other interfaces	Serial RS-232	D-SUB 9 connector 3 digital inputs and 3 digital outputs	Serial RS-232	D-SUB 9 connector 3 digital inputs and 3 digital outputs
Memory	128-Mbyte RAM	128-Mbyte Flash SD card Replaceable configuration memory	128-Mbyte RAM	128-Mbyte Flash SD card Replaceable configuration memory
Redundancy options	Optional: VPN	router and firewall	–
Power supply	Voltage range 11 ... 36 V DC, redundant	Voltage range 11 ... 36 V DC
Current consumption	Typical < 200 mA (24 V DC) | Maximum < 800 mA (10 V DC)	Typical < 200 mA (24 V DC) | Maximum < 800 mA (10 V DC)
Humidity range	5% ... 95% (operation, storage), non-condensing	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20	IP20
Temperature range	-20°C ... +60°C (operation) -20°C ... +70°C (storage)	-20°C ... +60°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	130 mm x 45 mm x 114 mm (up to DIN rail support)	130 mm x 45 mm x 114 mm (up to DIN rail support)
Weight	749 g (TX/DTX)	749 g (TX)
Weight (incl. packaging)	906 g (TX/DTX)	906 g (TX)

Firmware and power values	FL MGUARD RS4004	FL MGUARD RS2005
Firmware compatibility	Firmware 8.1.5: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.	
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: 120 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	
Virtual Private Network (VPN)	IPsec (IETF standard) Optionally up to 250 VPN tunnels	IPsec (IETF standard) Up to 2 VPN tunnels
Hardware-based encryption	DES	3DES	AES-128/192/256	DES	3DES	AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: 30 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 20 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	
Management support	Web GUI (HTTPS)	command line interface (SSH)	SNMP v1/2/3	central device management software	
Diagnostics	13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signal Status, SIM Status)	service I/O	log file	remote Syslog	

Other	FL MGUARD RS4004	FL MGUARD RS2005
Special features	Realtime clock	Trusted Platform Module (TPM)	temperature sensor	mGuard Secure Cloud ready	

4 TC MGUARD RS4000/RS2000 3G

Table 4-1 Currently available products

Product designation	Phoenix Contact order number
TC MGUARD RS4000 3G VPN	2903440
TC MGUARD RS2000 3G VPN	2903441

Product description

The **TC MGUARD RS4000 3G** is suitable for distributed protection of production cells or individual machines against manipulation.

It features a 4-port managed LAN switch and an industrial 3G mobile communication modem for GPRS, UMTS, and CDMA networks with a download speed of up to 14.4 Mbps.

The mobile communication interface can be switched to WAN interface as redundancy path. A dedicated DMZ port with its own firewall rules enables segmentation and differentiated security concepts. The GPS/GLONASS receiver enables time synchronization and location services. You can integrate automation devices with serial interfaces into networks, as a COM server is integrated.

For software-independent remote maintenance, the TC MGUARD RS4000 3G can be used as a VPN router for up to 10 (optionally up to 250) parallel, IPsec-encrypted VPN tunnels.

The **TC MGUARD RS2000 3G** is a version with basic firewall and can be used as a VPN client for up to two parallel, IPsec-encrypted VPN tunnels. It is suitable for secure remote maintenance applications at locations without wired networks and enables global connection of distributed machines and controllers.

Both versions support a replaceable configuration memory in the form of an SD card. To increase security, VPN connections can be switched on or off via switch contact, SMS or software interface. The fanless metal housing is mounted on a DIN rail.

Figure 4-1 TC MGUARD RS2000 3G/TC MGUARD RS4000 3G

4.1 Operating elements and LEDs

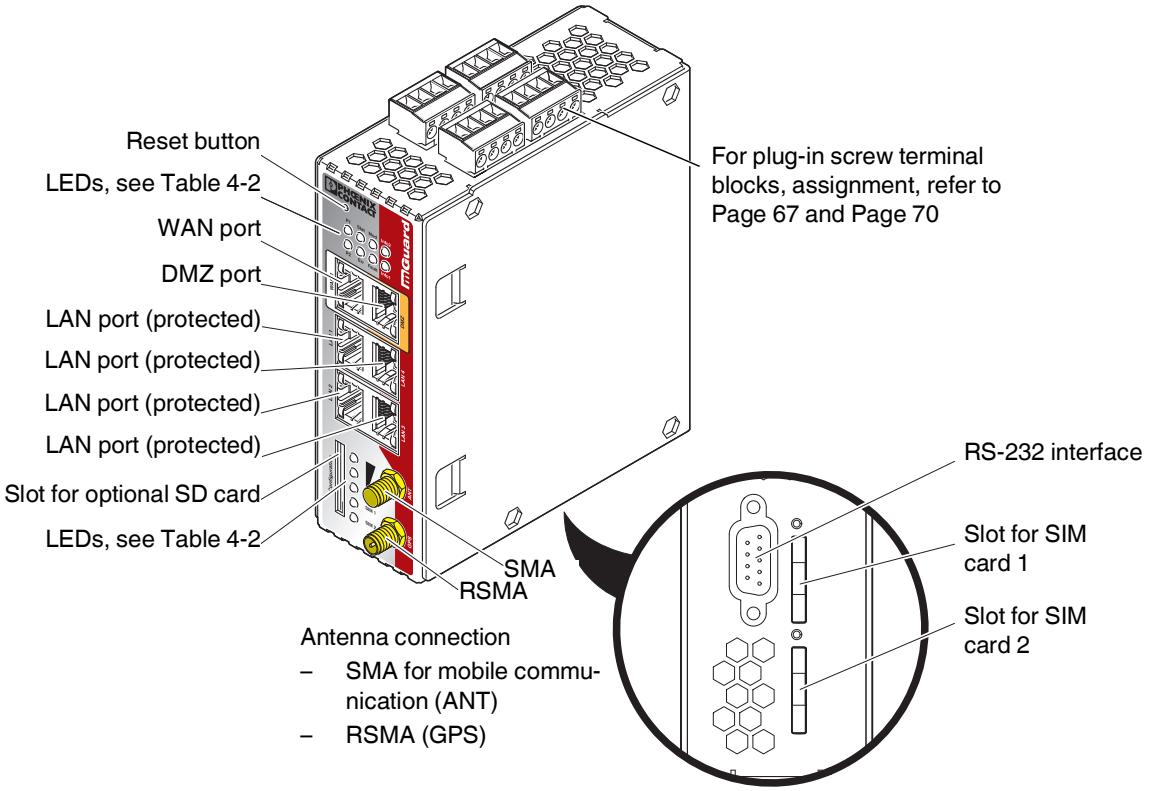


Figure 4-2 Operating elements and LEDs on the TC MGUARD RS4000 3G

Table 4-2 LEDs on the TC MGUARD RS4000 3G and TC MGUARD RS2000 3G

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active (TC MGUARD RS2000 3G: not used)
Stat	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
Err	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see Page 77) or contact your dealer.
Stat + Err	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
Mod	Green	On	Connection via modem established
Fault	Red	On	The signal output changes to the low level due to an error (inverted control logic). The signal output is inactive during a restart.

Table 4-2 LEDs on the TC MGUARD RS4000 3G and TC MGUARD RS2000 3G [...]

LED	State		Meaning			
Info2	Green	On	Up to firmware version 8.0		As of firmware version 8.1	
			The configured VPN connection has been established at output O1.		The configured VPN connections are established at output O1 or the firewall rule records defined at output O1 are activated.	
		Flashing	The configured VPN connection is being established or aborted at output O1.		The configured VPN connections are being established or aborted at output O1 or the firewall rule records defined at output O1 are activated or deactivated.	
Info1	Green	On	Up to firmware version 8.0		As of firmware version 8.1	
			The configured VPN connection has been established at output O2.		The configured VPN connections are established at output O2 or the firewall rule records defined at output O2 are activated.	
		Flashing	The configured VPN connection is being established or aborted at output O2.		The configured VPN connections are being established or aborted at output O2 or the firewall rule records defined at output O2 are activated or deactivated.	
WAN 1[1]	Green	On	The LEDs are located in the sockets (10/100 and duplex LED)			
DMZ1	Green	On	**Ethernet status**. The LEDs indicate the status of the relevant port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN, WAN or DMZ. When data packets are transmitted, the LED goes out briefly.			
LAN 1–4	Green	On				
Bar graph	LED 3	Top	Off	Off	Off	Green
	LED 2	Middle	Off	Off	Green	Green
	LED 1	Bottom	Off	Yellow	Yellow	Yellow
	Signal strength		-113 ... 111 dBm	-109 ... 89 dBm	-87 ... 67 dBm	-65 ... 51 dBm
	Network reception		Very poor to none	Sufficient	Good	Very good
SIM 1	Green	On	SIM card 1 active			
		Flashing	No PIN or incorrect one entered			
SIM 2	Green	On	SIM card 2 active			
		Flashing	No PIN or incorrect one entered			

[1] only TC MGUARD RS4000 3G

4.2 Startup

4.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

For connecting a modem or serial terminal to the RS-232 interface, you will need a null modem cable not exceeding 10 m in length.

NOTE: Risk of material damage due to emissions

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.

NOTE: Electrostatic discharge

When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) according to EN 61340-5-1 and IEC 61340-5-1.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature: -40°C ... +60°C
– Maximum humidity, non-condensing: 5% ... 95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Extended run-up time at low temperatures

Low temperatures result in a prolonged run-up time of the device. Operational availability is reached after a maximum of 5 minutes.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

4.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– The device
– Package slip
– Plug-in screw terminal blocks for the power supply connection and inputs/outputs (inserted)

4.2.3 mGuard-Firmware

– The device must be operated with mGuard firmware version 8.0 or higher.

4.3 Installation of TC MGUARD RS4000/RS2000 3G

4.3.1 Mounting/removal

NOTE: Device damage
Only mount and remove devices when the power supply is disconnected.

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Mount the TC MGUARD RS4000/RS2000 3G on a grounded 35 mm DIN rail according to DIN EN 60715.

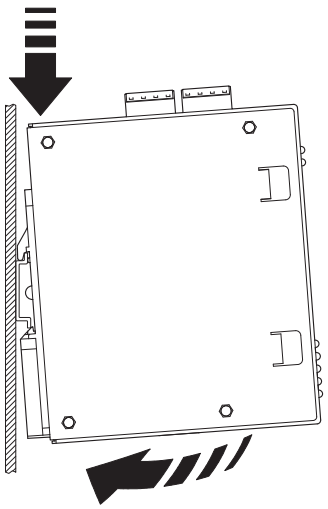


Figure 4-3 Mounting the TC MGUARD RS4000/RS2000 3G on a DIN rail

- Attach the top snap-on foot of the TC MGUARD RS4000/RS2000 3G to the DIN rail and then press the TC MGUARD RS4000/RS2000 3G down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the TC MGUARD RS4000/RS2000 3G from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the TC MGUARD RS4000/RS2000 3G.

4.3.2 Connecting to the network

NOTE: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply. Use UTP cables with an impedance of 100 Ω.
- Connect the internal network interface LAN of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

4.3.3 Connecting service contacts

NOTE: Do **not** connect the voltage and ground outputs to an external source.

The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.

The TC MGUARD RS4000/RS2000 3G has three digital inputs and outputs. These are configured in the web interface, e.g., the starting and stopping of VPN, sending alarms via SMS etc..

The digital inputs and outputs are connected as follows.

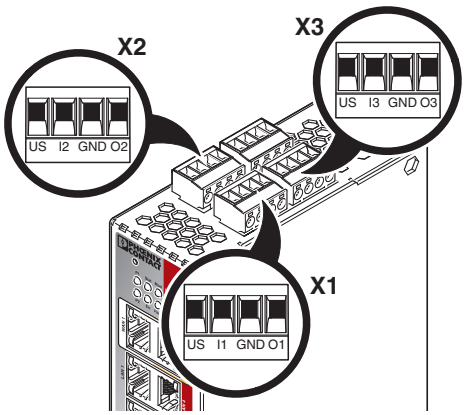
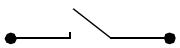
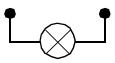


Figure 4-4 Service contacts

	Control switch CMD		Signal output (digital) ACK	
	US	**I1, I2, I3**	**GND**	**O1, O2, O3**
X1 ... X3	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switch output, maximum 250 mA at 11 ... 36 V DC
	Example 		Example 	

A **push button** or an **on/off switch** (e.g., key switch) can be connected between **service contacts US and I.**

The **service contacts O1–O3** are non-floating, continuously short-circuit-proof and supply a maximum of 250 mA.

The switching inputs and switching outputs can be connected with signals from external devices, e.g., with PLC signals. In this case, ensure the same potential as well as voltage and current specifications are defined.

Depending on the firmware version used, the service contacts can be used for various switching or signaling tasks.

4.3.4 Antennas

To establish a mobile communication connection, a matching **antenna** must be connected to the devices.

NOTE: Health effects due to RF radiation

A distance of at least 20 cm between persons and the antennas must be maintained during normal operation.

NOTE: Removing operator permissions

Operation of the wireless system is only permitted with accessories supplied by Phoenix Contact. The use of other accessory components may invalidate the operating license.

You can find the approved accessories for this wireless system listed with the product at: phoenixcontact.net/products.

We recommend combined mobile phone GPS antenna with omnidirectional characteristic, antenna cable with SMA round plug (GSM/UMTS) and R-SMA round plug (TC ANT MOBILE/GPS, 2903590 from Phoenix Contact).

In the case of the **TC MGUARD RS2000 3G**, the WAN is only available via the mobile network, as a WAN interface is not available. The mobile network function is preset. The TC MGUARD RS2000 3G can only be operated in Router mode.

Connecting antennas

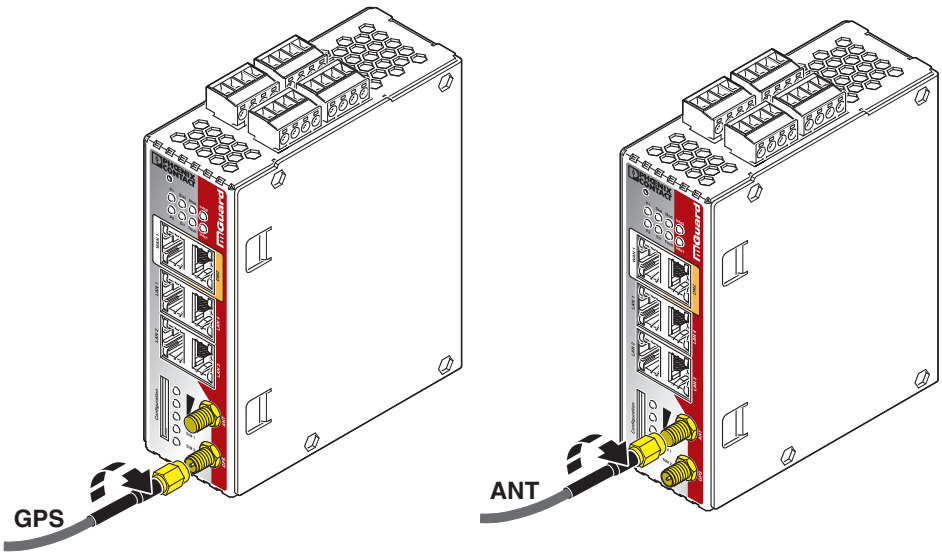


Figure 4-5 Antenna connection

- Connect one or two suitable antenna to the antenna connection.
  Antenna connection
  - SMA for mobile communication (ANT)
  - RSMA (GPS)
- If the bar graph indicates good or very good reception, affix the antenna (see “Bar graph” on page 63).

4.3.5 SIM card

To establish a mobile communication connection, the device also requires at least one valid **mini SIM card** in ID-000 format, via which it assigns and authenticates itself to a mobile network.

The TC MGUARD RS4000/RS2000 3G can be equipped with two SIM cards. The SIM card in the SIM 1 slot is the primary SIM card which is normally used to establish the connection. If this connection fails, the device can optionally turn to the second SIM card in slot SIM 2. You can set whether, and under which conditions, the connection to the primary SIM card is restored.

The state of the SIM cards is indicated via two LEDs on the front. The LEDs SIM1 and SIM2 light up green when the SIM card is active. If a PIN has not been entered, the LED flashes green.

Quality of the mobile network connection

The signal strength of the mobile network connection is indicated by three LEDs on the front of the TC MGUARD RS4000/RS2000 3G. The LEDs function as a bar graph (refer to “Bar graph” on page 63).

For stable data transmission, we recommend at least good network reception. If the network reception is only adequate, only SMS messages can be sent and received.

Inserting the SIM card

You will receive a SIM card from the wireless provider on which all data and services for your connection are stored. If you use CDMA networks in the USA (e.g., from Verizon Wireless), you will not receive a SIM card. Change the TC MGUARD RS4000/RS2000 3G to a CDMA provider via the web interface.

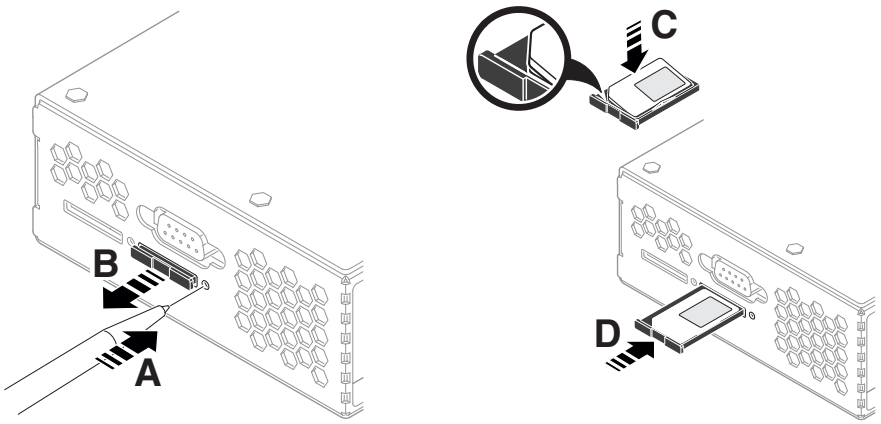


Figure 4-6 Insert the SIM card

To insert the SIM card, proceed as follows:

- Press the release button.
- Remove the SIM card holder.
- Insert the SIM card so that the SIM chip remains visible.
- Insert the SIM card holder together with the SIM card into the device until this ends flush with the housing.

4.3.6 Connecting the supply voltage

WARNING: The device is designed for operation with a DC voltage of 11 V DC ... 36 V DC/SELV, 800 mA maximum.

Therefore, only SELV circuits with voltage limitations according to IEC 60950/EN 60950/VDE 0805 may be connected to the supply connections and the signal contact.

The supply voltage is connected via a plug-in screw terminal block, which is located on the top of the device.

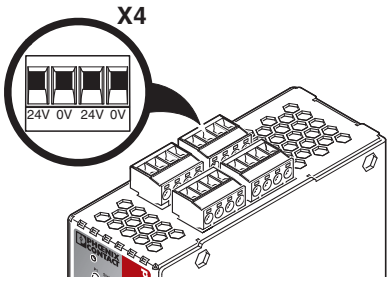
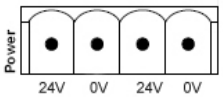
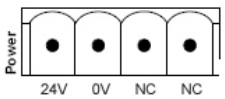


Figure 4-7 Connecting the supply voltage (TC MGUARD RS4000 3G)

Table 4-3 Supply voltage TC MGUARD RS4000/RS2000 3G

TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
	

The TC MGUARD RS4000 3G has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Wire the supply voltage lines of the X4 mGuard screw terminal block. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the plug-in screw terminal blocks into the intended sockets on the top of the device.

Status LED P1 lights up green when the supply voltage has been connected properly. On the TC MGUARD RS4000 3G, the status indicator P2 also lights up if there is a redundant supply voltage connection.

The device boots the firmware. The Stat LED flashes green. The device is ready for operation as soon as the Ethernet socket LEDs light up. Additionally, the P1/P2 LEDs light up green and Stat LED flashes green at heartbeat.

Redundant voltage supply (TC MGUARD RS4000 3G)

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the TC MGUARD RS4000 3G alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the TC MGUARD RS4000 3G indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs or by installing an appropriate wire jumper between the connections.

4.4 Preparing the configuration

4.4.1 Connection requirements

– The **TC MGUARD RS4000/RS2000 3G** must be connected to at least one active power supply unit.
– **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
– **For remote configuration**: The device must be configured so that remote configuration is permitted.
– The device must be connected, i.e., the required connections must be working.

4.5 Configuration in Router mode

On initial startup, the device can be accessed via the following address:
– https://192.168.1.1

4.5.1 IP address 192.168.1.1

In Router mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.
– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:
- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

4.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via the following address:

Table 4-4 Preset address

Default setting	Network mode	Management IP #1 (IP address of the internal interface)
TC MGUARD RS4000 3G	Router	https://192.168.1.1/
TC MGUARD RS2000 3G	Router	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 4-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 77).

If the administrator web page is not displayed

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

- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.

  Click on “Properties” under “LAN settings”.

  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 4-8 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

4.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

4.8 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

4.9 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

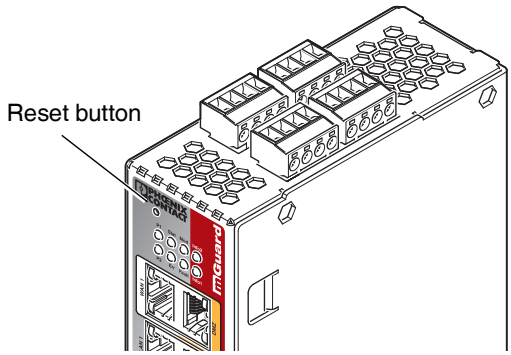


Figure 4-9 Reset button

4.9.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the Err LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

4.9.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

When performing the recovery procedure, the default network settings are established:

Table 4-5 Preset address

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

The device is reset to router mode with the fixed IP address.

- The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
- In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
- The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

- The device is in Router or PPPoE mode.
- The configured IP address of the device differs from the default setting.
- The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 4-6 Preset address

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately two seconds, the Stat LED lights up green.

- When the Stat LED has gone out, slowly press the Reset button again six times.
  If successful, the Stat LED lights up green.
  If unsuccessful, the Err LED lights up red.

If successful, the device restarts after two seconds and switches to Router mode. The device can then be reached again under the corresponding address.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

4.9.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

– **All configured settings are deleted.** The device is set to the delivery state.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

– All necessary firmware files must be located in a common directory on the first partition of the SD card

– This partition must use a VFAT file system (standard type for SD cards).

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

– The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.

– This SD card has been inserted into the device.

– The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s
  Firmware/pxs8_03001_0100617.usf.xz.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the Stat, Mod, and Sig LEDs light up green. Then, the device is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**
  If the Reset button is not released, the device is restarted.
  The device now starts the rescue system: It searches for a DHCP server via the LAN interface in order to obtain an IP address. (Exception: if an SD card is inserted into the device with corresponding firmware, the rescue system is started from there).
  The Stat LED flashes.
  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.
  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.
  The Stat, Mod, and Sig LEDs form a running light.
  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.
  This process takes around 3 to 5 minutes. The Stat LED is lit continuously.
  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the Stat, Mod, and Sig LEDs flash green simultaneously.

- Restart the device. To do so, press the Reset button.
  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 73):

4.10 Technical data

Hardware properties	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Platform	Freescale network processor	Freescale network processor
Network interfaces	4 LAN Ports (managed) I 1 DMZ port I 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 I full duplex I auto MDIX	4 LAN ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ45 I full duplex I auto MDIX
Wireless interface	WAN I GSM I GPRS I EDGE I UMTS I CDMA2000	WAN I GSM I GPRS I EDGE I UMTS I CDMA2000
SIM interfaces (1 + 2)	1.8 V I 3 V, redundant	1.8 V I 3 V, redundant
Data rate	≤ 14.4 Mbps (HSDPA)	≤ 14.4 Mbps (HSDPA)
Other interfaces	Serial RS-232 I D-SUB 9 connector 3 digital inputs and 3 digital outputs	Serial RS-232 I D-SUB 9 connector 3 digital inputs and 3 digital outputs
Memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory
Redundancy options	Optional: VPN I router and firewall	–
Power supply	Voltage range 11 ... 36 V DC, redundant	Voltage range 11 ... 36 V DC, redundant
Power consumption	typical < 200 mA (24 V DC) I maximum < 800 mA (10 V DC)	typical < 200 mA (24 V DC) I maximum < 800 mA (10 V DC)
Humidity range	5% ... 95% (operation, storage), non-condensing	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20	IP20
Temperature range	-40°C ... +60°C (operation) -40°C ... +70°C (storage)	-40°C ... +60°C (operation) -40°C ... +70°C (storage)
Vibration resistance in acc. with EN 60068-2-6/IEC 60068-2-6	5g, 10-150 Hz, 2.5 h, in XYZ direction	5g, 10-150 Hz, 2.5 h, in XYZ direction
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)	130 x 45 x 114 mm (up to DIN rail support)
Weight	850 g	835 g

Firmware and power values	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Firmware compatibility	For mGuard v8.0 or later: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.	
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: 110 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	
Virtual Private Network (VPN)	IPsec (IETF standard) Optionally up to 250 VPN tunnels	IPsec (IETF standard) Up to 2 VPN tunnels
Hardware-based encryption	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: 30 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 20 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	
Data throughput (mobile)	Depending on the mobile connection ≤ 5,7 Mbit/s (HSDPA) upload ≤ 14,4 Mbit/s (HSDPA) download	
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software	
Diagnostics	13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signal Status, SIM Status) I Service I/OI Log File I Remote Syslog	

Emitted interference in acc. with EN 61000-6-4	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Radio interference voltage in acc. with EN 55011	EN 55011 class A industrial area of application	
Emitted radio interference in acc. with EN 55011	EN 55011 class A industrial area of application	
Noise emission	EN 61000-6-4	
Criterion A	Normal operating behavior within the specified limits	
Criterion B	Criterion B Temporary impairment of operating behavior that is corrected by the device itself	

Other	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Conformance	CE	FCC	UL 508	electrical isolation (VCC//PE)	ANSI / ISA 12.12 Class I Div. 2	
Special features	GPS/GLONASS receiver	realtime clock	Trusted Platform Module (TPM)	temperature sensor	mGuard Secure Cloud ready	

5 TC MGUARD RS4000/RS2000 4G

Table 5-1 Currently available products

Product designation	Phoenix Contact order number
TC MGUARD RS4000 4G VPN	2903586
TC MGUARD RS2000 4G VPN	2903588
TC MGUARD RS4000 4G VZW VPN	1010461 (Verizon Wireless – USA)
TC MGUARD RS2000 4G VZW VPN	1010462 (Verizon Wireless – USA)
TC MGUARD RS4000 4G ATT VPN	1010463 (AT&T – USA)
TC MGUARD RS2000 4G ATT VPN	1010464 (AT&T – USA)

Product description

The four device variants designed for the US market (**VZW** and **ATT**) can only be operated in the mobile networks of the mobile providers

– *Verizon Wireless* (TC MGUARD RS4000/RS2000 4G VZW VPN) respectively
– *AT&T* (TC MGUARD RS4000/RS2000 4G ATT VPN).

Figure 5-1 TC MGUARD RS4000 4G

The **TC MGUARD RS4000 4G** is suitable for distributed protection of production cells or individual machines against manipulation. It features a 4-port managed LAN switch and an industrial 4G mobile communication modem for

– **TC MGUARD RS4000 4G VPN**: GPRS, UMTS, LTE, and CDMA networks
– **TC MGUARD RS4000 4G VZW VPN**: LTE networks
– **TC MGUARD RS4000 4G ATT VPN**: UMTS and LTE networks

with a download speed of up to 150 Mbps.

The mobile communication interface can be switched to WAN interface as redundancy path. A dedicated DMZ port with its own firewall rules enables segmentation and differentiated security concepts. The GPS/GLONASS receiver enables time synchronization and location services (only the devices 2903586 and 2903588). You can integrate automation devices with serial interfaces into networks, as a COM server is integrated.

For software-independent remote maintenance, the TC MGUARD RS4000 4G can be used as a VPN router for up to 10 (optionally up to 250) parallel, IPsec-encrypted VPN tunnels.

The **TC MGUARD RS2000 4G** is a version with basic firewall and can be used as a VPN client for up to two parallel, IPsec-encrypted VPN tunnels. It is suitable for secure remote maintenance applications at locations without wired networks and enables global connection of distributed machines and controllers.

Mobile network support:

– **TC MGUARD RS2000 4G VPN**: GPRS, UMTS, LTE, and CDMA networks
– **TC MGUARD RS2000 4G VZW VPN**: LTE
– **TC MGUARD RS2000 4G ATT VPN**: UMTS, LTE

Both versions support a replaceable configuration memory in the form of an SD card. To increase security, VPN connections can be switched on or off via switch contact, SMS or software interface. The fanless metal housing is mounted on a DIN rail.

5.1 Operating elements and LEDs

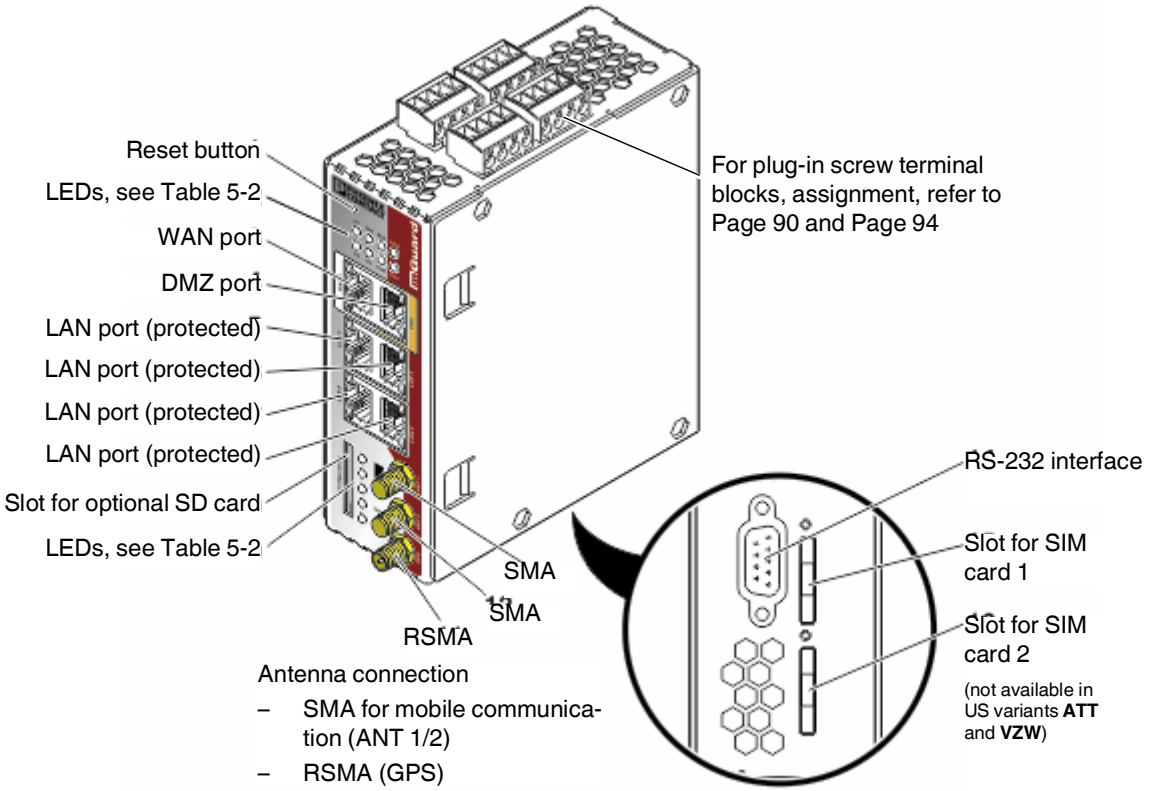


Figure 5-2 Operating elements and LEDs on the TC MGUARD RS4000 4G

Table 5-2 LEDs on the TC MGUARD RS4000 4G and TC MGUARD RS2000 4G

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active (TC MGUARD RS2000 4G: not used)
Stat	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
Err	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see Page 101) or contact your dealer.
Stat + Err	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
Mod	Green	On	Connection via modem established
Fault	Red	On	The signal output changes to the low level due to an error (inverted control logic). The signal output is inactive during a restart.

Table 5-2 LEDs on the TC MGUARD RS4000 4G and TC MGUARD RS2000 4G [...]

LED	State		Meaning			
Info2	Green	On	Up to firmware version 8.0		As of firmware version 8.1	
			The configured VPN connection has been established at output O1.		The configured VPN connections are established at output O1 or the firewall rule records defined at output O1 are activated.	
		Flashing	The configured VPN connection is being established or aborted at output O1.		The configured VPN connections are being established or aborted at output O1 or the firewall rule records defined at output O1 are activated or deactivated.	
Info1	Green	On	Up to firmware version 8.0		As of firmware version 8.1	
			The configured VPN connection has been established at output O2.		The configured VPN connections are established at output O2 or the firewall rule records defined at output O2 are activated.	
		Flashing	The configured VPN connection is being established or aborted at output O2.		The configured VPN connections are being established or aborted at output O2 or the firewall rule records defined at output O2 are activated or deactivated.	
WAN 1[1]	Green	On	The LEDs are located in the sockets (10/100 and duplex LED)			
DMZ1	Green	On	**Ethernet status**. The LEDs indicate the status of the relevant port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN, WAN or DMZ. When data packets are transmitted, the LED goes out briefly.			
LAN 1–4	Green	On				
Bar graph	LED 3	Top	Off	Off	Off	Green
	LED 2	Middle	Off	Off	Green	Green
	LED 1	Bottom	Off	Yellow	Yellow	Yellow
	Signal strength		-113 ... 111 dBm	-109 ... 89 dBm	-87 ... 67 dBm	-65 ... 51 dBm
	Network reception		Very poor to none	Sufficient	Good	Very good
SIM 1	Green	On	SIM card 1 active			
		Flashing	No PIN or incorrect one entered			
SIM 2 (not available in US variants **ATT** and **VZW**)	Green	On	SIM card 2 active			
		Flashing	No PIN or incorrect one entered			

[1] only TC MGUARD RS4000 4G

5.2 Startup

5.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

For connecting a modem or serial terminal to the RS-232 interface, you will need a null modem cable not exceeding 10 m in length.

NOTE: Risk of material damage due to emissions

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.

NOTE: Electrostatic discharge

When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) according to EN 61340-5-1 and IEC 61340-5-1.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  -40°C ... +60°C
– Maximum humidity, non-condensing:
  5% ... 95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Extended run-up time at low temperatures

Low temperatures result in a prolonged run-up time of the device. Operational availability is reached after a maximum of 5 minutes.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

5.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– The device
– Package slip
– Plug-in screw terminal blocks for the power supply connection and inputs/outputs (inserted)

5.2.3 mGuard-Firmware

– The device must be operated with mGuard firmware version 8.4 or higher.

5.3 Installation of TC MGUARD RS4000/RS2000 4G

5.3.1 Mounting/removal

NOTE: Device damage
Only mount and remove devices when the power supply is disconnected.

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Mount the TC MGUARD RS4000/RS2000 4G on a grounded 35 mm DIN rail according to DIN EN 60715.

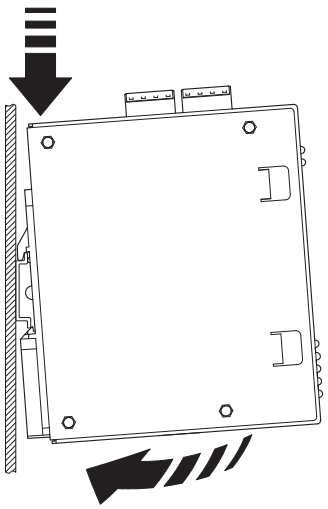


Figure 5-3 Mounting the TC MGUARD RS4000/RS2000 4G on a DIN rail

- Attach the top snap-on foot of the TC MGUARD RS4000/RS2000 4G to the DIN rail and then press the TC MGUARD RS4000/RS2000 4G down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the TC MGUARD RS4000/RS2000 4G from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the TC MGUARD RS4000/RS2000 4G.

5.3.2 Connecting to the network

NOTE: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply. Use UTP cables with an impedance of 100 Ω.
- Connect the internal network interface LAN of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

5.3.3 Connecting service contacts

NOTE: Do **not** connect the voltage and ground outputs to an external source.

The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.

The TC MGUARD RS4000/RS2000 4G has three digital inputs and outputs. These are configured in the web interface, e.g., the starting and stopping of VPN, sending alarms via SMS etc..

The digital inputs and outputs are connected as follows.

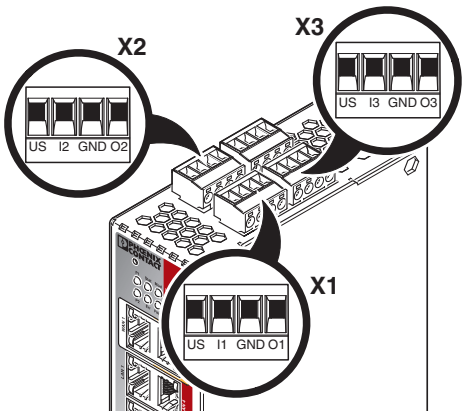
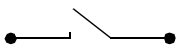
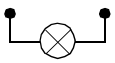


Figure 5-4 Service contacts

	Control switch CMD		Signal output (digital) ACK	
	US	**I1, I2, I3**	**GND**	**O1, O2, O3**
X1 ... X3	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switch output, maximum 250 mA at 11 ... 36 V DC
	Example 		Example 	

A **push button** or an **on/off switch** (e.g., key switch) can be connected between **service contacts US and I.**

The **service contacts O1–O3** are non-floating, continuously short-circuit-proof and supply a maximum of 250 mA.

The switching inputs and switching outputs can be connected with signals from external devices, e.g., with PLC signals. In this case, ensure the same potential as well as voltage and current specifications are defined.

Depending on the firmware version used, the service contacts can be used for various switching or signaling tasks.

5.3.4 Antennas

To establish a mobile communication connection, matching **antennas** must be connected to the devices.

TC MGUARD RS4000/RS2000 4G devices have two SMA round plugs for the antennas. For optimum LTE reception, always connect two antennas to the devices.

NOTE: Health effects due to RF radiation

A distance of at least 20 cm between persons and the antennas must be maintained during normal operation.

NOTE: Removing operator permissions

Operation of the wireless system is only permitted with accessories supplied by Phoenix Contact. The use of other accessory components may invalidate the operating license.

You can find the approved accessories for this wireless system listed with the product at: phoenixcontact.net/products.

We recommend the multiband mobile phone antenna with mounting bracket for outdoor installation (TC ANT MOBILE WALL 5M, Article No. 2702273). Also refer to the antenna documentation at phoenixcontact.net/product/2702273.

In the case of the **TC MGUARD RS2000 4G**, the WAN is only available via the mobile network, as a WAN interface is not available. The mobile network function is preset. The **TC MGUARD RS2000 4G** can only be operated in Router mode.

Connecting antennas

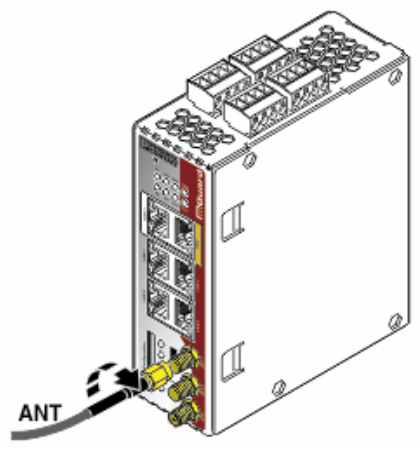


Figure 5-5 Antenna connection

- Connect two or three suitable antennas to the antenna connections:
  - Top and middle: SMA for mobile communication (ANT1/ANT2, primary/secondary antenna)
  - Bottom: RSMA (GPS)
- If the bar graph indicates good or very good reception, affix the antenna (see “Bar graph” on page 86).

5.3.5 SIM card

To establish a mobile communication connection, the device also requires at least one valid **mini SIM card** in ID-000 format, via which it assigns and authenticates itself to a mobile network.

The **TC MGUARD RS4000/RS2000 4G VPN** can be equipped with two SIM cards. The SIM card in the SIM 1 slot is the primary SIM card which is normally used to establish the connection. If this connection fails, the device can optionally turn to the second SIM card in slot SIM 2. You can set whether, and under which conditions, the connection to the primary SIM card is restored.

The state of the SIM cards is indicated via two LEDs on the front. The LEDs SIM1 and SIM2 light up green when the SIM card is active. If a PIN has not been entered, the LED flashes green.

The devices **TC MGUARD RS4000/RS2000 4G ATT VPN** and **VZW VPN** can only be operated with a single SIM card in the primary SIM card slot (SIM 1).

Quality of the mobile network connection

The signal strength of the mobile network connection is indicated by three LEDs on the front of the TC MGUARD RS4000/RS2000 4G. The LEDs function as a bar graph (refer to “Bar graph” on page 86).

For stable data transmission, we recommend at least good network reception. If the network reception is only adequate, only SMS messages can be sent and received.

Inserting the SIM card

You will receive a SIM card from the wireless provider on which all data and services for your connection are stored. If you use CDMA networks in the USA (e.g., from Verizon Wireless), you will not receive a SIM card. Change the TC MGUARD RS4000/RS2000 4G to a CDMA provider via the web interface.

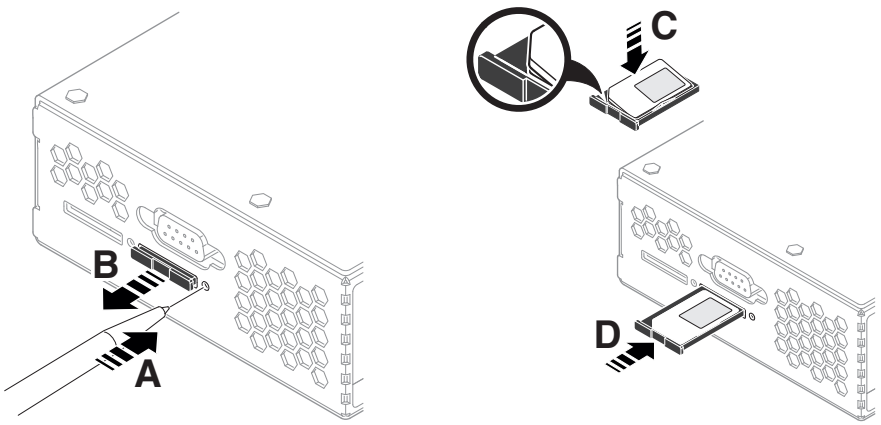


Figure 5-6 Insert the SIM card

To insert the SIM card, proceed as follows:

- Press the release button.
- Remove the SIM card holder.
- Insert the SIM card so that the SIM chip remains visible.

- Insert the SIM card holder together with the SIM card into the device until this ends flush with the housing.

5.3.6 Connecting the supply voltage

WARNING: The device is designed for operation with a DC voltage of 11 V DC ... 36 V DC/SELV, 800 mA maximum.

Therefore, only SELV circuits with voltage limitations according to IEC 60950/EN 60950/VDE 0805 may be connected to the supply connections and the signal contact.

The supply voltage is connected via a plug-in screw terminal block, which is located on the top of the device.

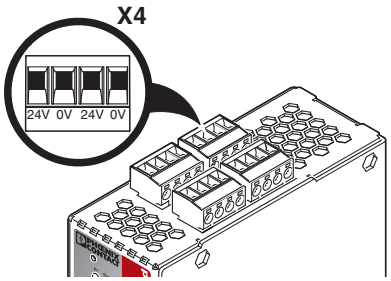
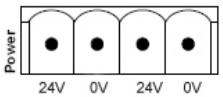
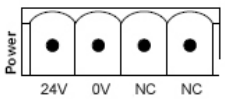


Figure 5-7 Connecting the supply voltage (TC MGUARD RS4000 4G)

Table 5-3 Supply voltage TC MGUARD RS4000/RS2000 4G

TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
	

The TC MGUARD RS4000 4G has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Wire the supply voltage lines of the X4 mGuard screw terminal block. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the plug-in screw terminal blocks into the intended sockets on the top of the device.

Status LED P1 lights up green when the supply voltage has been connected properly. On the TC MGUARD RS4000 4G, the status indicator P2 also lights up if there is a redundant supply voltage connection.

The device boots the firmware. The Stat LED flashes green. The device is ready for operation as soon as the Ethernet socket LEDs light up. Additionally, the P1/P2 LEDs light up green and Stat LED flashes green at heartbeat.

Redundant voltage supply (TC MGUARD RS4000 4G)

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the TC MGUARD RS4000 4G alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the TC MGUARD RS4000 4G indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs or by installing an appropriate wire jumper between the connections.

5.4 Preparing the configuration

5.4.1 Connection requirements

– The **TC MGUARD RS4000/RS2000 4G** must be connected to at least one active power supply unit.
– **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
– **For remote configuration**: The device must be configured so that remote configuration is permitted.
– The device must be connected, i.e., the required connections must be working.

5.5 Configuration in Router mode

On initial startup, the device can be accessed via the following address:
– https://192.168.1.1

5.5.1 IP address 192.168.1.1

In Router mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.
– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:
- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

5.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via the following address:

Table 5-4 Preset address

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 5-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 101).

If the administrator web page is not displayed

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

- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.

  Click on “Properties” under “LAN settings”.

  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

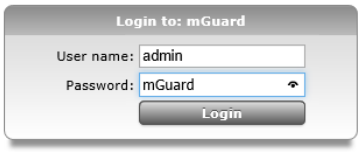


Figure 5-8 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

5.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

5.8 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

5.9 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

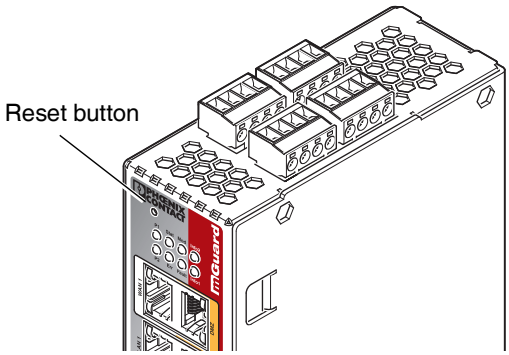


Figure 5-9 Reset button

5.9.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the Err LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

5.9.2 Performing a recovery procedure

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 5-5 Preset address

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately two seconds, the Stat LED lights up green.
- When the Stat LED has gone out, slowly press the Reset button again six times.
  If successful, the Stat LED lights up green.
  If unsuccessful, the Err LED lights up red.

If successful, the device restarts after two seconds and switches to Router mode. The device can then be reached again under the corresponding address.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

5.9.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

– **All configured settings are deleted.** The device is set to the delivery state.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

– All necessary firmware files must be located in a common directory on the first partition of the SD card

– This partition must use a VFAT file system (standard type for SD cards).

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

– The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.

– This SD card has been inserted into the device.

– The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:
  – Firmware/install-ubi.mpc83xx.p7s
  – Firmware/ubifs.img.mpc83xx.p7s
  – Firmware/ME909u-521_UPDATE_12.636.12.01.00.BIN.xz.p7s

In case of the devices **TC MGUARD RS4000/RS2000 4G ATT** and **VZW** the following firmware and modem firmware files must be used:

– **TC MGUARD RS4000/RS2000 4G ATT**:
  – install-ubi.mpc83xx.p7s
  – ubifs.img.mpc83xx.p7s
  – RHL75xx.A.2.11.151600.201709111842.x7160_8_signed_DWL.dwl.xz.p7s

– **TC MGUARD RS4000/RS2000 4G VZW**:
  – install-ubi.mpc83xx.p7s
  – ubifs.img.mpc83xx.p7s
  – RHL75xx.4.03.142600.201709280115.x7160_1_signed_DWL.dwl.xz.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the Stat, Mod, and Sig LEDs light up green. Then, the device is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**
  If the Reset button is not released, the device is restarted.
  The device now starts the rescue system: It searches for a DHCP server via the LAN interface in order to obtain an IP address. (Exception: if an SD card is inserted into the device with corresponding firmware, the rescue system is started from there).
  The Stat LED flashes.
  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.
  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.
  The Stat, Mod, and Sig LEDs form a running light.
  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.
  This process takes around 3 to 5 minutes. The Stat LED is lit continuously.
  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the Stat, Mod, and Sig LEDs flash green simultaneously.

- Restart the device. To do so, press the Reset button.
  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 97):

5.10 Technical data

Hardware properties	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Platform	Freescale network processor	Freescale network processor
Network interfaces	4 LAN Ports (managed) | 1 DMZ port | 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 | full duplex | auto MDIX	4 LAN ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ45 | full duplex | auto MDIX
Wireless interface (TC MGUARD RS4000/RS2000 4G VPN)	WAN | GSM | GPRS | EDGE | UMTS | LTE | CDMA2000	WAN | GSM | GPRS | EDGE | UMTS | LTE | CDMA2000
Wireless interface (TC MGUARD RS4000/RS2000 4G ATT VPN)	WAN | UMTS | LTE	WAN | UMTS | LTE
Wireless interface (TC MGUARD RS4000/RS2000 4G VZW VPN)	WAN | LTE	WAN | LTE
SIM interfaces (1 + 2)	1.8 V | 3 V, redundant	1.8 V | 3 V, redundant
SIM interfaces (1)	1.8 V | 3 V	1.8 V | 3 V
Data rate	≤ 14.4 Mbps (HSDPA)	≤ 14.4 Mbps (HSDPA)
Other interfaces	Serial RS-232 | D-SUB 9 connector 3 digital inputs and 3 digital outputs	Serial RS-232 | D-SUB 9 connector 3 digital inputs and 3 digital outputs
Memory	128 MB RAM | 128 MB Flash | SD card Replaceable configuration memory	128 MB RAM | 128 MB Flash | SD card Replaceable configuration memory
Redundancy options	Optional: VPN | router and firewall	–
Power supply	Voltage range 11 ... 36 V DC, redundant	Voltage range 11 ... 36 V DC, redundant
Power consumption	typical < 200 mA (24 V DC) | maximum < 800 mA (10 V DC)	typical < 200 mA (24 V DC) | maximum < 800 mA (10 V DC)
Humidity range	5% ... 95% (operation, storage), non-condensing	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20	IP20
Temperature range	-40°C ... +60°C (operation) -40°C ... +70°C (storage)	-40°C ... +60°C (operation) -40°C ... +70°C (storage)
Vibration resistance in acc. with EN 60068-2-6/IEC 60068-2-6	5g, 10-150 Hz, 2.5 h, in XYZ direction	5g, 10-150 Hz, 2.5 h, in XYZ direction
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)	130 x 45 x 114 mm (up to DIN rail support)
Weight	850 g	835 g

Firmware and power values	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Firmware compatibility	TC MGUARD RS4000/RS2000 4G VPN: mGuard v8.4.1 or later (0x3800 / 0x3900) TC MGUARD RS4000/RS2000 4G VPN: mGuard v8.8.4 or later (0x3880 / 0x3980) TC MGUARD RS4000/RS2000 4G ATT and VZW VPN: v8.7.0 oder later Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.	
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: 110 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	
Virtual Private Network (VPN)	IPsec (IETF standard) Optionally up to 250 VPN tunnels	IPsec (IETF standard) Up to 2 VPN tunnels
Hardware-based encryption	DES | 3DES | AES-128/192/256	DES | 3DES | AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: 30 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 20 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	

Firmware and power values	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Data throughput (mobile)	Depending on the mobile connection ≤ 50 Mbit/s (LTE) upload ≤ 150 Mbit/s (LTE) download	
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software	
Diagnostics	13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signal Status, SIM Status) I Service I/OI Log File I Remote Syslog	

Emitted interference in acc. with EN 61000-6-4	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Radio interference voltage in acc. with EN 55011	EN 55011 class A industrial area of application	
Emitted radio interference in acc. with EN 55011	EN 55011 class A industrial area of application	
Noise emission	EN 61000-6-4	
Criterion A	Normal operating behavior within the specified limits	
Criterion B	Criterion B Temporary impairment of operating behavior that is corrected by the device itself	

Other	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Conformance	CE I electrical isolation (VCC//PE)	
Special features	GPS/GLONASS receiver I Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Secure Cloud ready	

6 FL MGUARD RS2000 TX/TX-B

Table 6-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD RS2000 TX/TX-B	2702139

Product description

The **FL MGUARD RS2000 TX/TX-B** is an industrial router which offers static routing, NAT routing, 1:1 NAT routing, and port forwarding functions.

The device supports a replaceable configuration memory in the form of an SD card (an SD card is not supplied as standard). The fanless metal housing is mounted on a DIN rail.

Figure 6-1 FL MGUARD RS2000 TX/TX-B

6.1 Operating elements and LEDs

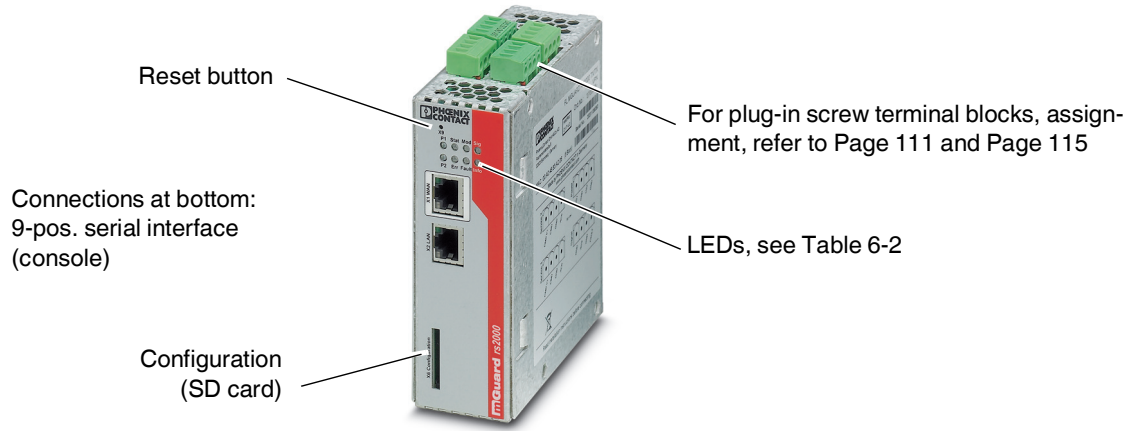


Figure 6-2 Operating elements and LEDs on the FL MGUARD RS2000 TX/TX-B

Table 6-2 LEDs on the FL MGUARD RS2000 TX/TX-B

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	Off	Redundant supply not provided
STAT	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
ERR	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see Page 120) or contact your dealer.
STAT+ ERR	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
SIG	–		(Not used)
FAULT	Red	On	The signal output is open due to an error at “low” signal (see Page 113). The signal output is inactive during a restart.
MOD	Green	Off	(Connection via modem is not provided)
INFO	Green	Off	(VPN connection is not provided)
LAN	Green	On	The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED)
WAN	Green	On	**Ethernet status**: Indicates the status of the LAN or WAN port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN or WAN. When data packets are transmitted, the LED goes out briefly.

6.2 Startup

6.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  -20°C ... +60°C
– Maximum humidity, non-condensing:
  5% ... 95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

6.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– The device
– Package slip
– Plug-in screw terminal blocks for the power supply connection and inputs/outputs (inserted)

6.3 Installation of FL MGUARD RS2000 TX/TX-B

6.3.1 Mounting/removal

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Mount the FL MGUARD RS2000 TX/TX-B on a grounded 35 mm DIN rail according to DIN EN 60715.

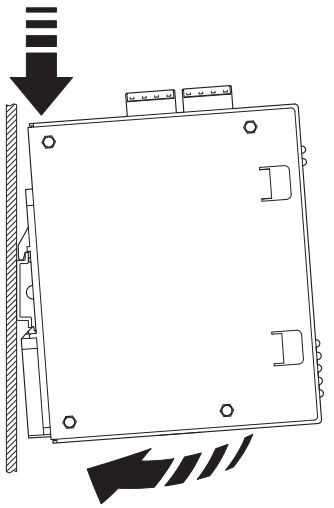


Figure 6-3 Mounting the FL MGUARD RS2000 TX/TX-B on a DIN rail

- Attach the top snap-on foot of the FL MGUARD RS2000 TX/TX-B to the DIN rail and then press the FL MGUARD RS2000 TX/TX-B down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the FL MGUARD RS2000 TX/TX-B from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the FL MGUARD RS2000 TX/TX-B.

6.3.2 Connecting to the network

NOTE: Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

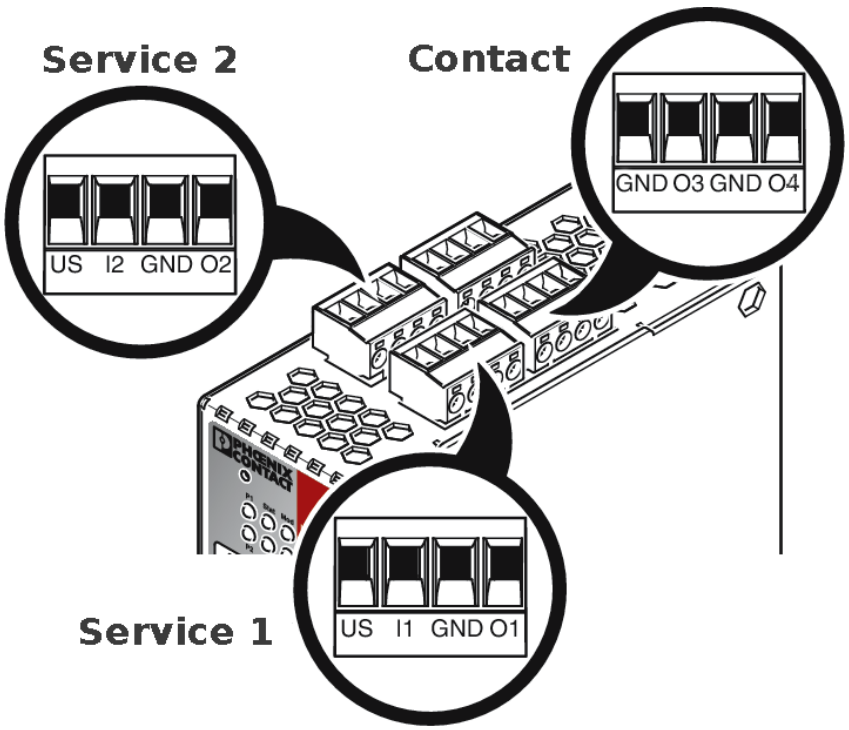
- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply.
- Connect the internal network interface LAN 1 of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

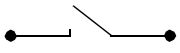
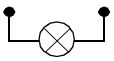
6.3.3 Service contacts

NOTE: Do **not** connect the voltage and ground outputs **US** (resp. **CMD V+**) and **GND** to an external voltage source.

Please note that only the “Service 1” contacts are used with firmware version up to and including 7.6.x. The “Service 2” contacts shall be made available as of firmware version 8.1.

The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.



	US	I1/I2	GND	O1/O2
Service 1 + 2	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output *
	Example 		Example 	

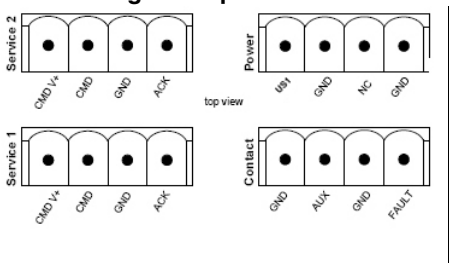
	24V	0V	NC	NC
Power	+24 V	0 V	+24 V	0 V
	See Section 6.3.4		Only for FL MGUARD RS4000 See Section 6.3.4	

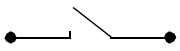
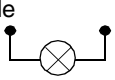
	GND	O3	GND	O4
Contact	Not used	Not used	Signal output (-)	Signal output (+)†

* Maximum of 250 mA at 11 ... 36 V DC

† 11 V ... 36 V when operating correctly; disconnected in the event of a fault

The following description of the contacts is also possible:



	CMD V+	CMD	GND	ACK
Service 1 + 2	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output *
	Example 		Example 	

	US1	GND	NC	GND
Power	+24 V	0 V	+24 V	0 V
	See Section 6.3.4		Only for FL MGUARD RS4000 See Section 6.3.4	

	GND	AUX	GND	FAULT
Contact	Not used	Not used	Signal output (-)	Signal output (+)†

* Maximum of 250 mA at 11 ... 36 V DC

† 11 V ... 36 V when operating correctly; disconnected in the event of a fault

A **push button** or an **on/off switch** (e.g., key switch) can be connected between **service contacts US** and **I** (resp. CMD V+ and CMD).

The **contacts O1/O2 (+)** and **O4 (+)** (resp. ACK and FAULT) are non-floating, continuously short-circuit-proof and supply a maximum of 250 mA.

The switching inputs and switching outputs can be connected with signals from external devices, e.g., with signals from PLCs. In this case, ensure the same potential as well as voltage and current specifications are defined.

Depending on the firmware version used, the service contacts can be used for various switching or signaling tasks.

Service contacts as of firmware version 8.1

Input/CMD I1, CMD I2

Via the web interface under “Management, Service I/O”, you can set whether a push button or an on/off switch has been connected to the inputs. One or more freely selectable VPN connections or firewall rule records can be switched via the corresponding switch. A mixture of VPN connections and firewall rule records is also possible. The web interface displays which VPN connections and which firewall rule records are connected to this input.

The push button or on/off switch is used to establish and release predefined VPN connections or the defined firewall rule records.

Operating a connected push button

- To switch on the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.
- To switch off the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.

Operating a connected on/off switch

- To switch on the selected VPN connections or firewall rule records, set the switch to ON.
- To switch off the selected VPN connections or firewall rule records, set the switch to OFF.

Signal contact (signal output) O1, O2 resp. ACK

Via the web interface under “Management, Service I/O” you can set whether certain VPN connections or firewall rule records are monitored and displayed via the LED Info 1 (output/O1 resp. ACK) or LED Info 2 (output/O2 resp. ACK).

If VPN connections are being monitored, an illuminated Info LED indicates that VPN connections are established.

Alarm output O4 resp. FAULT

The O4 alarm output monitors the function of the device and therefore enables remote diagnostics.

The Fault LED lights up red if the signal output changes to the low level due to an error (inverted control logic).

The O4 alarm output reports the following when “Management, Service I/O, Alarm output” has been activated.

– Monitoring of the link status of the Ethernet connections
– Monitoring of the temperature condition
– Monitoring of the connection state of the internal modem

Service contacts up to firmware version 8.0

Signal contact (signal output)

The signal contact monitors the function of the FL MGUARD RS2000 TX/TX-B and thus enables remote diagnostics.

The FAULT LED lights up red if the signal output is open due to an error.

The voltage at the signal contact corresponds to the supply voltage applied. The following is reported when monitoring the output voltage:

– Failure of the supply voltage.
– Power supply of the FL MGUARD RS2000 TX/TX-B below the limit value (supply voltage lower than 11 V).
– Link status monitoring of the Ethernet connections, if configured. By default upon delivery, the connection is not monitored. Monitoring can be activated (on the web interface under “Management >> System Settings >> Signal Contact”).
– Error during selftest.

During a restart, the signal contact is switched off until the FL MGUARD RS2000 TX/TX-B has started up completely. This also applies when the signal contact is manually set to “Closed” under “Manual settings” in the software configuration.

6.3.4 Connecting the supply voltage

WARNING: The FL MGUARD RS4000/RS2000 is designed for operation with a DC voltage of 11 V DC ... 36 V DC/SELV, 1.5 A, maximum.

Therefore, only SELV circuits with voltage limitations according to EN 60950-1 may be connected to the supply connections and the signal contact.

The supply voltage is connected via a plug-in screw terminal block, which is located on the top of the device.

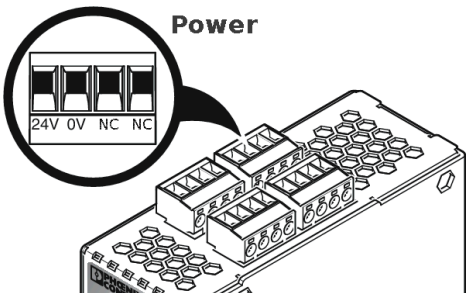


Figure 6-4 Connecting the supply voltage

Instead of the designation **24V** the designation **US1** is also used.

Status LED P1 lights up green when the supply voltage has been connected properly.

The device boots the firmware. Status LED STAT flashes green. The device is ready for operation as soon as the Ethernet socket LEDs light up. Additionally, status LED P1 lights up green and status LED STAT flashes green at heartbeat.

6.4 Preparing the configuration

6.4.1 Connection requirements

– The **FL MGUARD RS2000 TX/TX-B** must be connected to an active power supply unit.
– **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
– The device must be connected, i.e., the required connections must be working.

6.4.2 Local configuration on startup

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following addresses:

Table 6-3 Preset addresses

Default setting	Network mode	Management IP #1 (IP address of the internal interface)
FL MGUARD RS2000 TX/TX-B	Router	https://192.168.1.1/

6.4.3 IP address 192.168.1.1

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

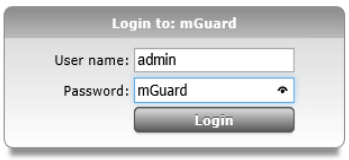


Figure 6-5 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

6.5 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

6.6 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

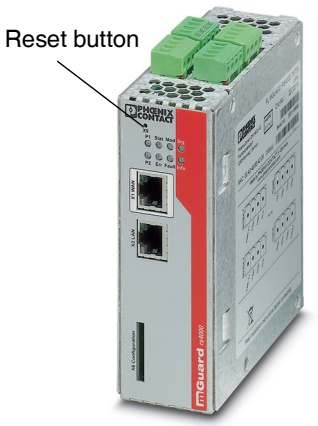


Figure 6-6 Reset button

6.6.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the ERR LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

6.6.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

When performing the recovery procedure, the default network settings are established:

Table 6-4 Preset addresses

Default setting	Network mode	Management IP #1 (IP address of the internal interface)
FL MGUARD RS2000 TX/TX-B	Router	https://192.168.1.1/

The device is reset to Router mode with the default settings.

– In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).

Possible reasons for performing the recovery procedure:

– The configured IP address of the device differs from the default setting.

– The current IP address of the device is not known.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 6-5 Preset addresses

Default setting	Network mode	Management IP #1 (IP address of the internal interface)
FL MGUARD RS2000 TX/TX-B	Router	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately 2 seconds, the STAT LED lights up green.
- Press the Reset button slowly again six times.
  If successful, the STAT LED lights up green.
  If unsuccessful, the ERR LED lights up red.

If successful, the device restarts after two seconds and switches to Stealth mode. The device can then be reached again under the corresponding addresses.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

6.6.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

– **All configured settings are deleted.** The device is set to the delivery state.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

– All necessary firmware files must be located in a common directory on the first partition of the SD card.

– This partition must use a VFAT file system (standard type for SD cards).

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

– The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.

– This SD card has been inserted into the device.

– The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s

  Firmware/ubifs.img.mpc83xx.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the STAT, MOD, and SIG LEDs light up green. Then, the device is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**
  If the Reset button is not released, the device is restarted.
  The device now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.
  The STAT LED flashes.
  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.
  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.
  The STAT, MOD, and SIG LEDs form a running light.
  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.
  This process takes around 3 to 5 minutes. The STAT LED is lit continuously.
  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the STAT, MOD, and SIG LEDs flash green simultaneously.

- Restart the device. To do this, briefly press the Reset button.
  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. You can now configure it again (see “After successful connection establishment” on page 117):

- Switch to the “TFTP Server” or “DHCP Server” tab page and click on “Settings” to set the parameters as follows:

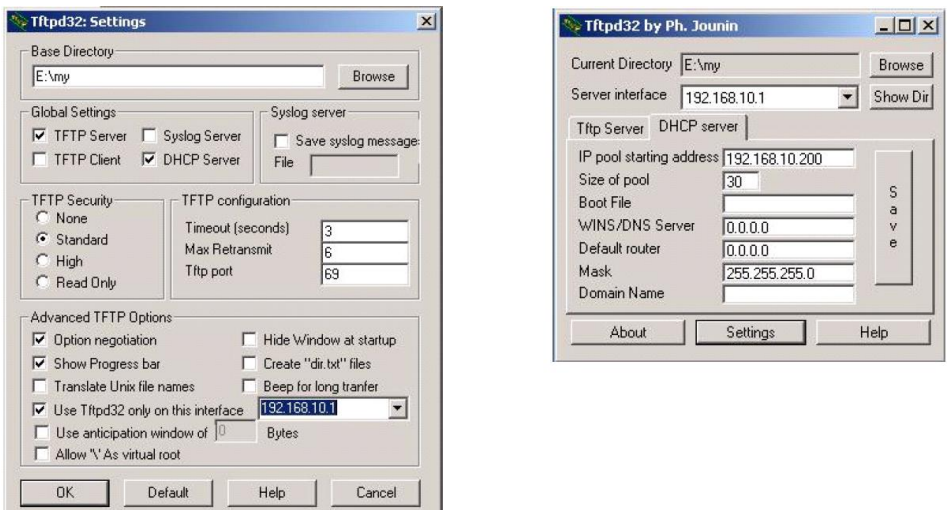


Figure 6-7 Settings

Under Linux

All current Linux distributions include DHCP and TFTP servers.

- Install the corresponding packages according to the instructions provided for the relevant distribution.
- 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**

- 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:
install.p7s, jffs2.img.p7s

- If a major release upgrade of the firmware is carried out by flashing, the license file purchased for the upgrade must also be stored here under the name **licence.lic**.

  Make sure that this is the correct license file for the device (under “Management >> Update” on the web interface).
- Then restart the inetd process to apply the configuration changes.
- When using a different mechanism, e.g., xinetd, please consult the relevant documentation.

6.7 Technical data

Hardware properties	FL MGUARD RS2000 TX/TX-B
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232 D-SUB 9 plug 2 digital inputs and 2 digital outputs (not all used)
Memory	128 MB RAM I 128 MB Flash SD card Replaceable configuration memory
High availability options	None
Power supply	Voltage range 11 ... 36 V DC
Power consumption	2.13 W, typical
Humidity range	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20
Temperature range	-20°C ... +60°C (operation) -20°C ... +60°C (storage)
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)
Weight	725 g
Weight (incl. packaging)	900 g

Firmware and power values	FL MGUARD RS2000 TX/TX-B
Firmware compatibility	mGuard v8.x or later: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput	Bidirectional throughput: 120 Mbps, maximum
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) signal contacts I service contacts I log file I remote syslog

Other	FL MGUARD RS2000 TX/TX-B
Conformance	CE I UL 508
Special features	Realtime clock I temperature sensor

7 FL MGUARD RS4000 TX/TX-P

Table 7-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD RS4000 TX/TX-P	2702259

Product description

The **FL MGUARD RS4000 TX/TX-P** is a security router with intelligent firewall and IPsec VPN (up to 250 tunnels). Providing a special DPI (Deep Packet Inspection) functionality for OPC Classic and Modbus TCP, it has been designed for use in the process industry to accommodate strict distributed security and high availability requirements.

The FL MGUARD RS4000 TX/TX-P supports a replaceable configuration memory in the form of an SD card. (The SD cards are not supplied as standard.) The fanless metal housing is mounted on a DIN rail.

Figure 7-1 FL MGUARD RS4000 TX/TX-P

DPI for OPC Classic

Deep Package Inspection for OPC Classic analyzes the transmitted packets, and modifies them, if necessary. The device can be configured so that only OPC packets can be sent via OPC Classic port 135. Deep Packet Inspection reliably detects the TCP ports negotiated between the devices during the connection opened first.

Exactly these ports are then opened through the firewall, and enabled for OPC communication. If no OPC packets are transmitted via these ports within a configurable timeout, the ports are closed again. By means of fine-tuned firewall rules, it can be defined exactly which clients may or may not communicate with which servers via OPC. This Connection Tracking function significantly enhances the security level.

DPI for Modbus TCP

The device can inspect packets of incoming and outgoing Modbus TCP connections and filter them if required. The user data of incoming packets is inspected.

7.1 Operating elements and LEDs

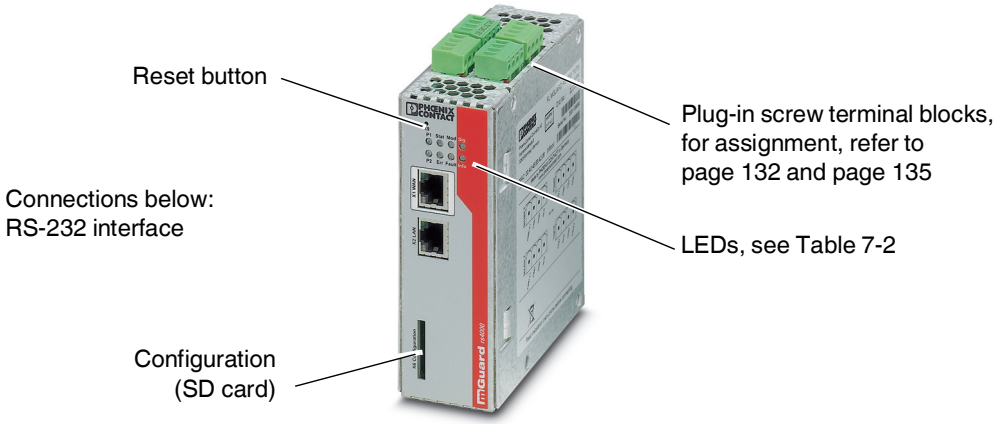


Figure 7-2 Operating elements and LEDs on the FL MGUARD RS4000 TX/TX-P

Table 7-2 LEDs on the FL MGUARD RS4000 TX/TX-P

LED	Status		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active
STAT	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
ERR	Red	Flashing	**System error**. Restart the device. – Press the reset button shortly (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see page 143) or contact your dealer.
STAT+ ERR	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
SIG	–		(Not used)
FAULT	Red	On	The signal output changes to the low level due to an error (inverted control logic) (see page 134). The signal output is inactive during a restart.
MOD	Green	On	Connection via modem established

Table 7-2 LEDs on the FL MGUARD RS4000 TX/TX-P[...]

LED	Status		Meaning
INFO	Green	On	Up to firmware version 8.0: the configured VPN connection has been established As of firmware version 8.1, the configured VPN connections are established or the firewall rule records defined at output O1 are activated
		Flashing	Up to firmware version 8.0: the configured VPN connection is being established or aborted As of firmware version 8.1: the configured VPN connections are being established or aborted or the defined firewall rule records are activated or deactivated.
LAN	Green	On	The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED)
WAN	Green	On	**Ethernet status**. Indicates the status of the LAN or WAN port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN or WAN. When data packets are transmitted, the LED goes out briefly.

7.2 Startup

7.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature: –40°C...+70°C
– 5 %... 95% relative humidity, temporary condensation according to 3K7/IEC EN 60721-3-3 (except for wind-driven precipitation and ice buildup)

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

7.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– Device
– Package slip
– Plug-in screw terminal blocks for the power supply connection and inputs/outputs (inserted)

7.3 Installation of FL MGUARD RS4000 TX/TX-P

7.3.1 Mounting/removal

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Mount the FL MGUARD RS4000 TX/TX-P on a grounded 35 mm DIN rail according to DIN EN 60715.

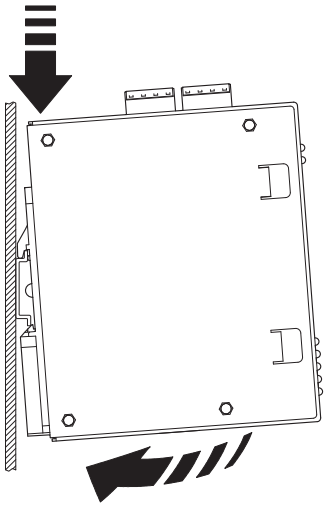


Figure 7-3 Mounting the FL MGUARD RS4000 TX/TX-P on a DIN rail

- Attach the top snap-on foot of the FL MGUARD RS4000 TX/TX-P to the DIN rail and then press the FL MGUARD RS4000 TX/TX-P down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the FL MGUARD RS4000 TX/TX-P from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the FL MGUARD RS4000 TX/TX-P.

7.3.2 Connecting to the network

NOTE: Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

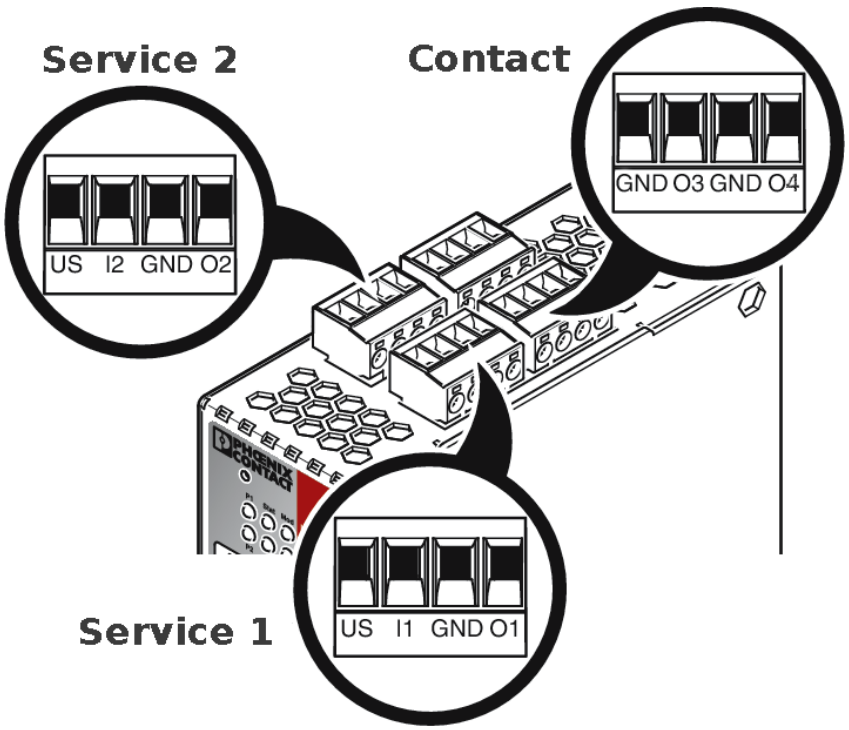
- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply.
- Connect the internal network interface LAN 1 of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

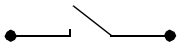
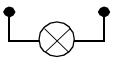
7.3.3 Service contacts

NOTE: Do **not** connect the voltage and ground outputs **US** (resp. **CMD V+**) and **GND** to an external voltage source.

Please note that only the “Service 1” contacts are used with firmware version up to and including 7.6.x. The “Service 2” contacts shall be made available as of firmware version 8.1.

The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.



Service 1 + 2	US	I1/I2	GND	O1/O2
	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output *
	Example 		Example 	

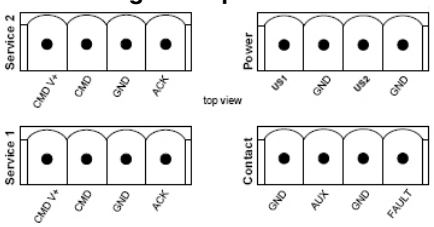
Power	24V	0V	24V	0V
	+24 V	0 V	+24 V	0 V
	See section 7.3.4		Only for FL MGUARD RS4000 See section 7.3.4	

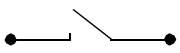
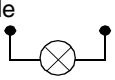
Contact	GND	O3	GND	O4
	Not used	Not used	Signal output (-)	Signal output (+)†

* Maximum of 250 mA at 11 ... 36 V DC

† 11 V ... 36 V when operating correctly; disconnected in the event of a fault

The following description of the contacts is also possible:



Service 1 + 2	CMD V+	CMD	GND	ACK
	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output *
	Example 		Example 	

Power	US1	GND	US2	GND
	+24 V	0 V	+24 V	0 V
	See section 7.3.4		Only for FL MGUARD RS4000 See section 7.3.4	

Contact	GND	AUX	GND	FAULT
	Not used	Not used	Signal output (-)	Signal output (+)†

* Maximum of 250 mA at 11 ... 36 V DC

† 11 V ... 36 V when operating correctly; disconnected in the event of a fault

A **push button** or an **on/off switch** (e.g., key switch) can be connected between **service contacts US** and **I** (resp. CMD V+ and CMD).

The **contacts O1/O2 (+)** and **O4 (+)** (resp. ACK and FAULT) are non-floating, continuously short-circuit-proof and supply a maximum of 250 mA.

The switching inputs and switching outputs can be connected with signals from external devices, e.g., with signals from PLCs. In this case, ensure the same potential as well as voltage and current specifications are defined.

Depending on the firmware version used, the service contacts can be used for various switching or signaling tasks.

Service contacts as of firmware version 8.1

Input/CMD I1, CMD I2

Via the web interface under “Management, Service I/O”, you can set whether a push button or an on/off switch has been connected to the inputs. One or more freely selectable VPN connections or firewall rule records can be switched via the corresponding switch. A mixture of VPN connections and firewall rule records is also possible. The web interface displays which VPN connections and which firewall rule records are connected to this input.

The push button or on/off switch is used to establish and release predefined VPN connections or the defined firewall rule records.

Operating a connected push button

- To switch on the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.
- To switch off the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.

Operating a connected on/off switch

- To switch on the selected VPN connections or firewall rule records, set the switch to ON.
- To switch off the selected VPN connections or firewall rule records, set the switch to OFF.

Signal contact (signal output) O1, O2 resp. ACK

Via the web interface under “Management, Service I/O” you can set whether certain VPN connections or firewall rule records are monitored and displayed via the LED Info 1 (output/O1 resp. ACK) or LED Info 2 (output/O2 resp. ACK).

If VPN connections are being monitored, an illuminated Info LED indicates that VPN connections are established.

Alarm output O4 resp. FAULT

The O4 alarm output monitors the function of the FL MGUARD RS4000/RS2000 and therefore enables remote diagnostics.

The Fault LED lights up red if the signal output changes to the low level due to an error (inverted control logic).

The O4 alarm output reports the following when “Management, Service I/O, Alarm output” has been activated.

– Failure of the redundant supply voltage
– Monitoring of the link status of the Ethernet connections
– Monitoring of the temperature condition
– Monitoring of the redundancy status
– Monitoring of the connection state of the internal modem

7.3.4 Connecting the supply voltage

WARNING: The device is designed for operation at DC voltages of 11 V DC ... 36 V DC/SELV.

Therefore, only SELV circuits with voltage limitations according to IEC 60950/EN 60950/VDE 0805 may be connected to the supply connections and the signal contact.

The supply voltage is connected via a plug-in screw terminal block, which is located on the top of the device.

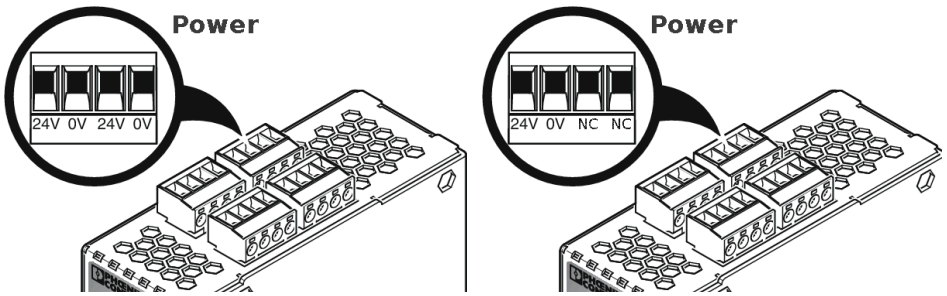


Figure 7-4 Connecting the supply voltage

Instead of the designation **24V/24V** the designation **US1/US2** is also used.

The device has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Do not connect the service contacts to an external voltage source.
- Wire the supply voltage lines with the corresponding screw terminal block **24V/24V** (resp. US1/US2) of the device. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the screw terminal blocks into the intended sockets on the top of the device (see Figure 7-4).

Status LED P1 lights up green when the supply voltage has been connected properly. On the device, the status indicator P2 also lights up if there is a redundant supply voltage connection.

The device boots the firmware. Status STAT LED flashes green. The device is ready for operation as soon as the Ethernet socket LEDs light up. Additionally, status LEDs P1/P2 light up green and the status STAT LED flashes green at heartbeat.

Redundant voltage supply

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the device alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the device indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs **24V/24V** (resp. US1/US2)) or by installing an appropriate wire jumper between connections **24V and 24V** (resp. US1 and US2).

7.4 Preparing the configuration

7.4.1 Connection requirements

– The **FL MGUARD RS4000 TX/TX-P** must be connected to at least one active power supply unit.
– **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
– **For remote configuration**: The device must be configured so that remote configuration is permitted.
– The device must be connected, i.e., the required connections must be working.

7.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following addresses:

Table 7-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000 TX/TX-P	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is reset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see page 139). Alternatively, you can select a different stealth configuration or use another network mode.

7.5 Configuration in Stealth mode

On initial startup, the device can be accessed via two addresses:

– https://192.168.1.1/ (see page 137)
– https://1.1.1.1/ (see page 138)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 138).

The device can be accessed via https://192.168.1.1/ if the external network interface is not connected on startup.

Computers can access the device via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the device. For this purpose, the device with LAN port and WAN port must be integrated in an operational network in which the default gateway can be accessed via the WAN port.

– After access via IP address 192.168.1.1 and successful login, IP address 192.168.1.1 is set as a fixed management IP address.
– After access via IP address 1.1.1.1, or after IP address assignment via BootP, access via IP address 192.168.1.1 is no longer possible.

7.5.1 IP address 192.168.1.1

In Stealth mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.

– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure have been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the “Internet protocol Version 4 (TCP/IPv4)” menu item.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

7.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the device to be addressed via address **https://1.1.1.1/**, it must be connected to a configured network interface. This is the case if it is connected in an existing network connection and if the default gateway can be accessed via the WAN port of the device at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 139). Continue from this point.

After access via IP address 1.1.1.1, access via IP address 192.168.1.1 is no longer possible.

7.5.3 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.

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

Section 14.1 explains IP address assignment using the free Windows software “IP Assignment Tool” (IPAssign.exe).

Notes for BootP

During initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the device no longer sends BootP requests. Access via IP address 192.168.1.1 is then no longer possible.

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) must be performed.

7.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via one of the following addresses:

Table 7-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000 TX/TX-P	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 7-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is unknown, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 143).

If the administrator web page is not displayed

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

- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.

  Click on “Properties” under “LAN settings”.

  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

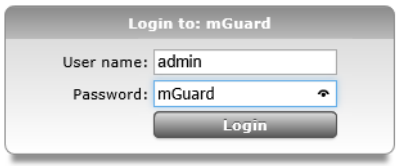


Figure 7-5 Login

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

User name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

7.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to software reference manual.

7.8 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

7.9 Restart, recovery procedure, and flashing the firmware

The reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

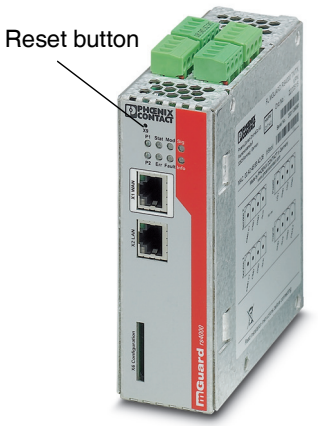


Figure 7-6 Reset button

7.9.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the ERR LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

7.9.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

Use the recovery procedure in case you have forgotten the IP address under which the device can be accessed.

The following network setting is restored:

Table 7-5 Restored network setting

Network mode	Management IP #1	Management IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is reset to Stealth mode with the default setting “multiple Clients”.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU configuration is activated for the Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The configured IP address of the device differs from the default setting.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 7-6 Restored network setting

Network mode	Management IP #1	Management IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the reset button six times.
  After approximately 2 seconds, the STAT LED lights up green.
- When the green STAT LED has gone out, slowly press the reset button again six times.
  If successful, the STAT LED lights up green.
  If unsuccessful, the ERR LED lights up red.

If successful, the device restarts after two seconds and switches to stealth mode. The device can then be reached again under the corresponding addresses.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

7.9.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

- **All configured settings are deleted.** The device is set to the delivery state.
- In mGuard firmware version 5.0.0 or later, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

- All necessary firmware files must be located in a common directory on the first partition of the SD card
- This partition must use a VFAT file system (standard type for SD cards)

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

- The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.
- This SD card has been inserted into the device.
- The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s

  Firmware/ubifs.img.mpc83xx.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the reset button until the STAT, MOD, and SIG LEDs light up green. The device then is in rescue status.
- **Release the reset button within one second of entering rescue status.**

  If the reset button is not released, the device is restarted.

  The device now starts the rescue system: It first searches for an inserted SD card and for the relevant firmware there. If the device does not find an SD card, it searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The STAT LED flashes.

  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.

  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.

  The STAT, MOD, and SIG LEDs form a running light.

  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.

  This process takes around 3 to 5 minutes. The STAT LED is lit continuously.

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the STAT, MOD, and SIG LEDs flash green simultaneously.

- Restart the device. To do so, press the reset button.

  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. Reconfigure it (see “Establishing a local configuration connection” on page 139).

7.10 Technical Data

Hardware properties	FL MGUARD RS4000 TX/TX-P
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232 I D-SUB 9 plug 2 digital inputs and 2 digital outputs each
Memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory
Redundancy options	VPN I router and firewall
Power supply	Voltage range 11 ... 36 V DC, redundant
Power consumption	2.13 W, typical
Humidity range	5 %... 95% (operation, storage), non-condensing
Degree of protection	IP20
Temperature range	-40°C... +70°C (operation) -40°C... +70°C (storage)
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)
Weight	730 g (TX/TX)
Weight (incl. packaging)	892 g (TX/TX)

Firmware and power values	FL MGUARD RS4000 TX/TX-P
Firmware compatibility	For mGuard v8.1.0 or newer: Phoenix Contact recommends the use of the latest firmware version and patch releases. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: max. 120 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 50 Mbps
Virtual Private Network (VPN)	IPsec (IETF standard) Up to 250 VPN tunnels
Hardware-based encryption	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rule, bidirectional throughput: max. 30 Mbps Stealth mode, default firewall rule, bidirectional throughput max. 20 Mbps
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) signal contacts I service contacts I log file I remote syslog

Miscellaneous	FL MGUARD RS4000 TX/TX-P
Conformance	CE I FCC I UL 508 ANSI/ISA 12.12 Class I Div. 2
Approvals	 Class I, Zone 2, Group IIC T4 Class I, Division 2, Groups A, B, C and D T4 **The following information applies when operating this equipment in hazardous locations:** – These devices must be installed in an enclosure rated IP54 and used in an area of not more than pollution degree 2. – Use 75°C copper conductors only. – Provisions shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 40%.
Further approvals	ISA-S71.04-1985 G3 Harsh Group A
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Remote Services Portal ready

8 FL MGUARD RS4000 TX/TX VPN-M

Table 8-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD RS4000 TX/TX VPN-M	2702465

Product description

The **FL MGUARD RS4000 TX/TX VPN-M** is a security router with intelligent firewall and IPsec VPN (10 tunnels / optionally up to 250 tunnels). It has been designed for use in industry to accommodate strict distributed security and high availability requirements.

The FL MGUARD RS4000 TX/TX VPN-M is functionally identical to the FL MGUARD RS4000. In contrast to the FL MGUARD RS4000 it has the approval for marine and offshore applications and an extended temperature range.

Current device specific information on the approval for marine and offshore applications can be found at phoenixcontact.net/product/2702465.

The FL MGUARD RS4000 TX/TX VPN-M support a replaceable configuration memory in the form of an SD card. (The SD cards are not supplied as standard.) The fanless metal housing is mounted on a DIN rail.

The following connectivity options are available:

FL MGUARD RS4000 TX/TX VPN-M: (LAN/WAN)

Ethernet/Ethernet + VPN

Figure 8-1 FL MGUARD RS4000 TX/TX VPN-M

8.1 Operating elements and LEDs

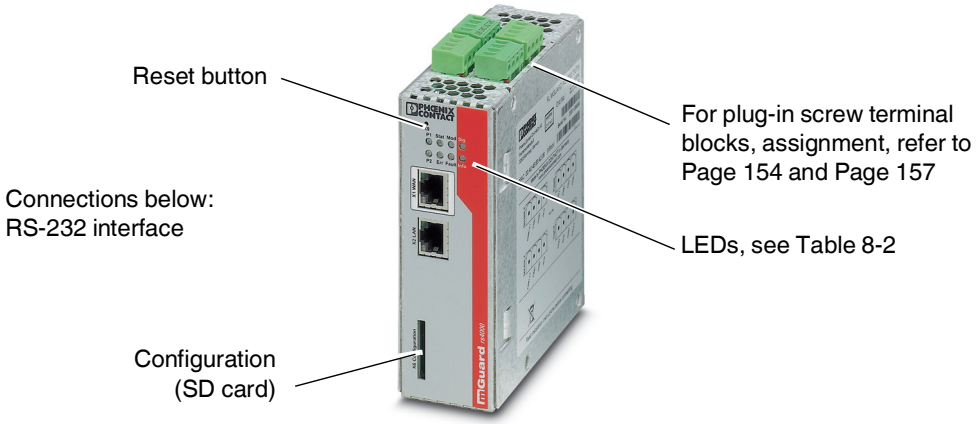


Figure 8-2 Operating elements and LEDs on the FL MGUARD RS4000 TX/TX VPN-M

Table 8-2 LEDs on the FL MGUARD RS4000 TX/TX VPN-M

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active
STAT	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
ERR	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see Page 166) or contact your dealer.
STAT+ ERR	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
SIG	–		(Not used)
FAULT	Red	On	The signal output changes to the low level due to an error (inverted control logic) (see Page 156). The signal output is inactive during a restart.
MOD	Green	On	Connection via modem established

Table 8-2 LEDs on the FL MGUARD RS4000 TX/TX VPN-M[...]

LED	State		Meaning
INFO	Green	On	Up to firmware version 8.0: the configured VPN connection has been established As of firmware version 8.1, the configured VPN connections are established or the firewall rule records defined at output O1 are activated
		Flashing	Up to firmware version 8.0: the configured VPN connection is being established or aborted As of firmware version 8.1: the configured VPN connections are being established or aborted or the defined firewall rule records are activated or deactivated.
LAN	Green	On	The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED)
WAN	Green	On	**Ethernet status.** Indicates the status of the LAN or WAN port. As soon as the device is connected to the relevant network, a continuous light indicates that there is a connection to the network partner in the LAN or WAN. When data packets are transmitted, the LED goes out briefly.

8.2 Startup

8.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  -40°C ... +70°C
– Maximum humidity, non-condensing
  5% ... 95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

8.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– The device
– Package slip
– Plug-in screw terminal blocks for the power supply connection and inputs/outputs (inserted)

8.3 Installation of FL MGUARD RS4000 TX/TX VPN-M

8.3.1 Mounting/removal

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Mount the device on a grounded 35 mm DIN rail according to DIN EN 60715.

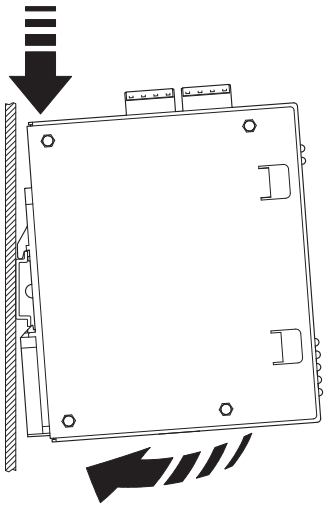


Figure 8-3 Mounting the device on a DIN rail

- Attach the top snap-on foot of the device to the DIN rail and then press the device down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the device from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the device.

8.3.2 Connecting to the network

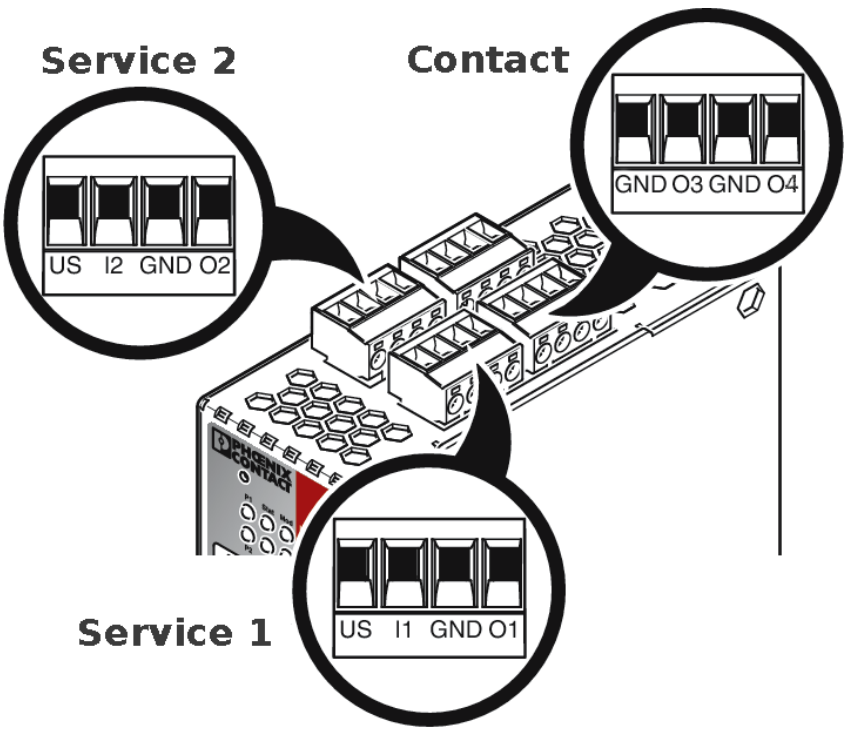
NOTE: Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

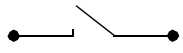
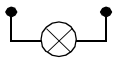
- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply.
- Connect the internal network interface LAN 1 of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

8.3.3 Service contacts

NOTE: Do **not** connect the voltage and ground outputs **US** (resp. **CMD V+**) and **GND** to an external voltage source.

The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.



	US	I1/I2	GND	O1/O2
Service 1 + 2	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output [1]
	Example 		Example 	

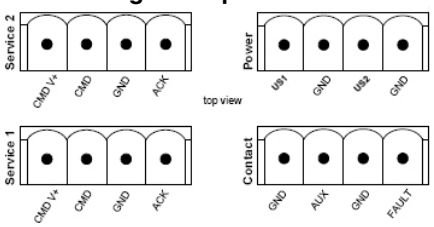
	24V	0V	24V	0V
Power	+24 V	0 V	+24 V	0 V
	See Section 8.3.4		Only for FL MGUARD RS4000 See Section 8.3.4	

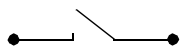
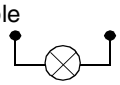
	GND	O3	GND	O4
Contact	Not used	Not used	Signal output (-)	Signal output (+)[2]

[1] Maximum of 250 mA at 11 ... 36 V DC

[2] 11 V ... 36 V when operating correctly; disconnected in the event of a fault

The following description of the contacts is also possible:



	CMD V+	CMD	GND	ACK
Service 1 + 2	Voltage output (+) Supply voltage	Switching input 11 ... 36 V DC	Ground output (-) Supply voltage	Short-circuit-proof switching output [1]
	Example 		Example 	

	US1	GND	US2	GND
Power	+24 V	0 V	+24 V	0 V
	See Section 8.3.4		Only for FL MGUARD RS4000 See Section 8.3.4	

	GND	AUX	GND	FAULT
Contact	Not used	Not used	Signal output (-)	Signal output (+)[2]

[1] Maximum of 250 mA at 11 ... 36 V DC

[2] 11 V ... 36 V when operating correctly; disconnected in the event of a fault

A **push button** or an **on/off switch** (e.g., key switch) can be connected between **service contacts US** and **I** (resp. CMD V+ and CMD).

The **contacts O1/O2 (+)** and **O4 (+)** (resp. ACK and FAULT) are non-floating, continuously short-circuit-proof and supply a maximum of 250 mA.

The switching inputs and switching outputs can be connected with signals from external devices, e.g., with signals from PLCs. In this case, ensure the same potential as well as voltage and current specifications are defined.

Depending on the firmware version used, the service contacts can be used for various switching or signaling tasks.

Service contacts as of firmware version 8.1

Input/CMD I1, CMD I2

Via the web interface under “Management, Service I/O”, you can set whether a push button or an on/off switch has been connected to the inputs. One or more freely selectable VPN connections or firewall rule records can be switched via the corresponding switch. A mixture of VPN connections and firewall rule records is also possible. The web interface displays which VPN connections and which firewall rule records are connected to this input.

The push button or on/off switch is used to establish and release predefined VPN connections or the defined firewall rule records.

Operating a connected push button

- To switch on the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.
- To switch off the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.

Operating a connected on/off switch

- To switch on the selected VPN connections or firewall rule records, set the switch to ON.
- To switch off the selected VPN connections or firewall rule records, set the switch to OFF.

Signal contact (signal output) O1, O2 resp. ACK

Via the web interface under “Management, Service I/O” you can set whether certain VPN connections or firewall rule records are monitored and displayed via the LED Info 1 (output/O1 resp. ACK) or LED Info 2 (output/O2 resp. ACK).

If VPN connections are being monitored, an illuminated Info LED indicates that VPN connections are established.

Alarm output O4 resp. FAULT

The O4 alarm output monitors the function of the FL MGUARD RS4000/RS2000 and therefore enables remote diagnostics.

The Fault LED lights up red if the signal output changes to the low level due to an error (inverted control logic).

The O4 alarm output reports the following when “Management, Service I/O, Alarm output” has been activated.

– Failure of the redundant supply voltage
– Monitoring of the link status of the Ethernet connections
– Monitoring of the temperature condition
– Monitoring of the redundancy status
– Monitoring of the connection state of the internal modem

8.3.4 Connecting the supply voltage

WARNING: The device is designed for operation at DC voltages of 11 V DC ... 36 V DC/SELV.

Therefore, only SELV circuits with voltage limitations according to IEC 60950/EN 60950/VDE 0805 may be connected to the supply connections and the signal contact.

The supply voltage is connected via a plug-in screw terminal block, which is located on the top of the device.

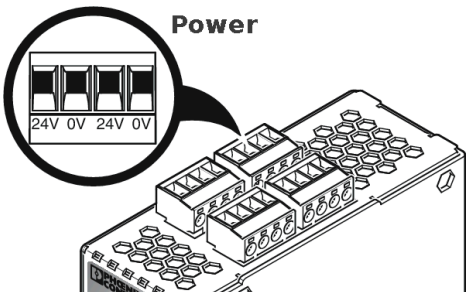


Figure 8-4 Connecting the supply voltage

Instead of the designation **24V/24V** the designation **US1/US2** is also used.

The device has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Do not connect the service contacts to an external voltage source.
- Wire the supply voltage lines with the corresponding screw terminal block **24V/24V** (resp. US1/US2) of the device. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the screw terminal blocks into the intended sockets on the top of the device (see Figure 8-4).

Status LED P1 lights up green when the supply voltage has been connected properly. On the device, the status indicator P2 also lights up if there is a redundant supply voltage connection.

The device boots the firmware. Status STAT LED flashes green. The device is ready for operation as soon as the Ethernet socket LEDs light up. Additionally, status LEDs P1/P2 light up green and the status STAT LED flashes green at heartbeat.

Redundant voltage supply

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the device alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the device indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs **24V/24V** (resp. US1/US2)) or by installing an appropriate wire jumper between connections **24V and 24V** (resp. US1 and US2).

8.4 Preparing the configuration

8.4.1 Connection requirements

– The **device** must be connected to at least one active power supply unit.
– **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
– **For remote configuration**: The device must be configured so that remote configuration is permitted.
– The device must be connected, i.e., the required connections must be working.

8.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following addresses:

Table 8-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000 TX/TX VPN-M	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 162). Alternatively, you can select a different stealth configuration or use another network mode.

8.5 Configuration in Stealth mode

On initial startup, the device can be accessed via two addresses:

– https://192.168.1.1/ (see Page 160)
– https://1.1.1.1/ (see Page 160)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 161).

The device can be accessed via https://192.168.1.1/ if the external network interface is not connected on startup.

Computers can access the device via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the device. For this purpose, the device with LAN port and WAN port must be integrated in an operational network in which the default gateway can be accessed via the WAN port.

– After access via IP address 192.168.1.1 and successful login, IP address 192.168.1.1 is set as a fixed management IP address.
– After access via IP address 1.1.1.1 or after IP address assignment via BootP, the product can no longer be accessed via IP address 192.168.1.1.

8.5.1 IP address 192.168.1.1

In Stealth mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.

– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

8.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the device to be addressed via address **https://1.1.1.1/,** it must be connected to a configured network interface. This is the case if it is connected in an existing network connection and if the default gateway can be accessed via the WAN port of the device at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 162). Continue from this point.

After access via IP address 1.1.1.1, the product can no longer be accessed via IP address 192.168.1.1

8.5.3 Assigning the IP address via BootP

After assigning an IP address via BootP, the product can no longer be accessed via IP address 192.168.1.1

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

Section 14.1 explains IP address assignment using the free Windows software "IP Assignment Tool" (IPAssign.exe).

Notes for BootP

During initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the device no longer sends BootP requests. The product 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) must be performed.

8.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via one of the following addresses:

Table 8-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000 TX /TX VPN-M	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 8-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 166).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 158).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.

  Click on “Properties” under “LAN settings”.

  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 8-5 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

8.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

8.8 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

8.9 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

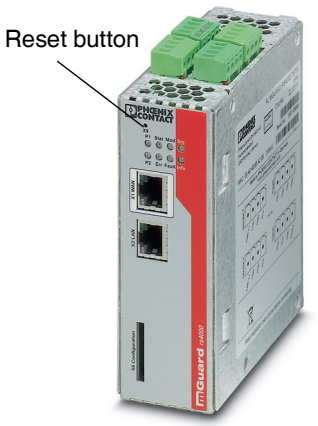


Figure 8-6 Reset button

8.9.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the ERR LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

8.9.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

When performing the recovery procedure, the default network settings are established:

Table 8-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000 TX/TX VPN-M	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is reset to Stealth mode with the default setting “multiple Clients”.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The configured IP address of the device differs from the default setting.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 8-6 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000 TX/TX VPN-M	Stealth	https://1.1.1.1/	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately 2 seconds, the STAT LED lights up green.
- Press the Reset button slowly again six times.
  If successful, the STAT LED lights up green.
  If unsuccessful, the ERR LED lights up red.

If successful, the device restarts after two seconds and switches to Stealth mode. The device can then be reached again under the corresponding addresses.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

8.9.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

- **All configured settings are deleted.** The device is set to the delivery state.
- In Version mGuard firmware version 5.0.0 or later, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

- All necessary firmware files must be located in a common directory on the first partition of the SD card
- This partition must use a VFAT file system (standard type for SD cards).

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

- The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.
- This SD card has been inserted into the device.
- The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s

  Firmware/ubifs.img.mpc83xx.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the STAT, MOD, and SIG LEDs light up green. Then, the device is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the device is restarted.

  The device now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The STAT LED flashes.

  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.

  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.

  The STAT, MOD, and SIG LEDs form a running light.

  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.

  This process takes around 3 to 5 minutes. The STAT LED is lit continuously.

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the STAT, MOD, and SIG LEDs flash green simultaneously.

- Restart the device. To do this, briefly press the Reset button.

  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 162).

8.10 Technical data

Hardware properties	FL MGUARD RS4000 TX/TX VPN-M
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232 I D-SUB 9 connector 2 digital inputs and 2 digital outputs
Memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory
Redundancy options	Optional: VPN I router and firewall
Power supply	Voltage range 11 ... 36 V DC, redundant
Power consumption	2.13 W, typical
Humidity range	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20
Temperature range	-40°C ... +70°C (operation) -40°C ... +70°C (storage)
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)
Weight	725 g (TX/TX)
Weight (incl. packaging)	900 g (TX/TX)

Firmware and power values	FL MGUARD RS4000 TX/TX VPN-M
Firmware compatibility	For mGuard v8.1.8 or later: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: 120 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum.
Virtual Private Network (VPN)	IPsec (IETF standard) Optionally up to 250 VPN tunnels
Hardware-based encryption	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: 30 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 20 Mbps, maximum
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) signal contacts I service contacts I log file I remote syslog

Other	FL MGUARD RS4000 TX/TX VPN-M
Conformance	CE I FCC I UL 508 ANSI/ISA 12.12 Class I Div. 2
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Remote Services Portal ready

9 FL MGUARD GT/GT

Table 9-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD GT/GT	2700197
FL MGUARD GT/GT VPN	2700198

Product description

The **FL MGUARD GT/GT** supports hybrid use as a router/firewall/VPN router both via Ethernet and for serial dial-up connections. The device is designed for DIN rail mounting (according to DIN EN 60715) and is therefore ideal for use in industrial applications.

VPN tunnels can be initiated using software or hardware switches. A redundant supply voltage can be connected (9 V DC ... 36 V DC).

The FL MGUARD GT/GT is available in two device versions:

– As a security appliance FL MGUARD GT/GT
– As a security appliance with VPN support FL MGUARD GT/GT VPN

To aid understanding, FL MGUARD GT/GT is used for the two device versions in this user manual. The properties described also apply to the FL MGUARD GT/GT VPN. Differences from the FL MGUARD GT/GT are indicated, if applicable.

Figure 9-1 FL MGUARD GT/GT

9.1 Operating elements and LEDs

9.1.1 Status and diagnostics indicators

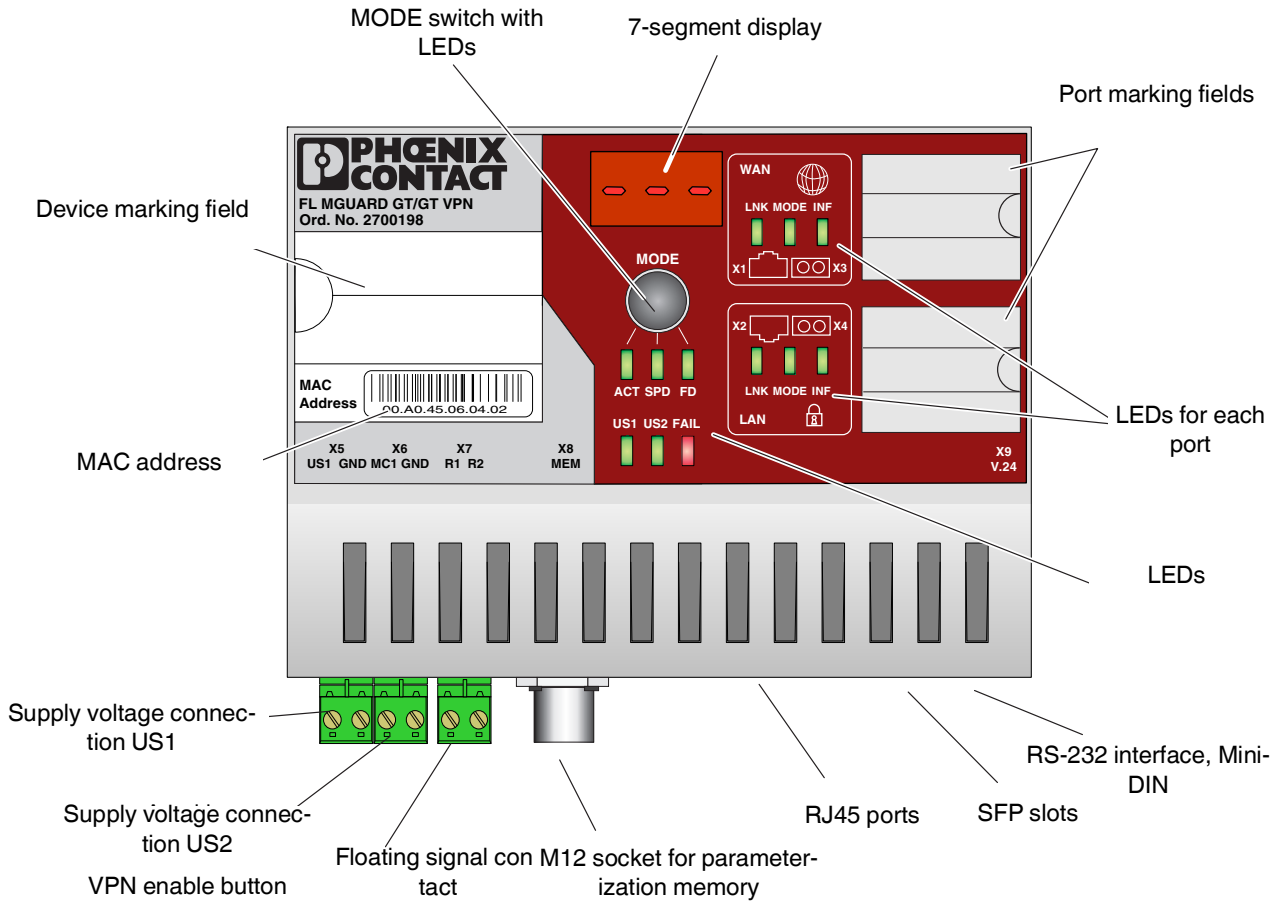


Figure 9-2 Operating elements and LEDs on the FL MGUARD GT/GT

Table 9-2 LEDs on the FL MGUARD GT/GT

LED	State		Meaning
US1	Green	On	Supply voltage 1 within the tolerance range
		Off	Supply voltage 1 too low
US2	Green	On	Supply voltage 2 within the tolerance range
		Off	Supply voltage 2 too low
FAIL	Red	On	Signal contact open, i.e., an error has occurred
		Off	Signal contact closed, i.e., an error has not occurred
A Link LED is located on the front of the device for the LAN and WAN port.			
LNK (Link)	Green	On	Link active
		Off	Link not active

Table 9-2 LEDs on the FL MGUARD GT/GT [...]

LED	State		Meaning
Another LED is located on the front of the device for the LAN and WAN port. The function of the second LED (MODE) for each port can be set using the MODE switch (see also example below). There are three options (during the boot process the mode and port LEDs are permanently on):			
ACT (Activity)	Green	On	Receiving telegrams
		Off	Not receiving telegrams
SPD (Speed)	Green/ orange	On (orange)	1000 Mbps
		On (green)	100 Mbps (for RJ45 ports only)
		Off	10 Mbps if Link LED is active (for RJ45 ports only)
FD (Duplex)	Green	On	Full duplex
		Off	Half duplex
ACT/SPD/FD	Yellow	Flashing	The device is in Smart mode (see “Restart, recovery procedure, and flashing the firmware” on page 191)
INF (Duplex)	Green	On	VPN tunnel established
		Flashing	VPN tunnel initialized
		Off	No VPN tunnel

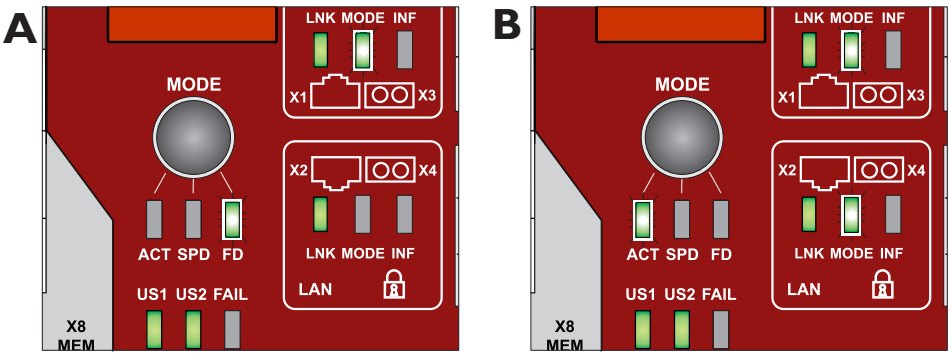


Figure 9-3 Example of FL MGUARD GT/GT status indicators

Example:

In Figure 9-3, the LED indicators have the following meaning:

A: The MODE switch has been set to display the duplex mode (FD); the mode LEDs now indicate that the LAN port is in half duplex mode and the WAN port is in full duplex mode.

B: The switch has been set to display the Activity (ACT); the mode LEDs now indicate that incoming data packets are detected on both ports.

9.1.2 Messages in the 7-segment display

During error-free operation:

Display	Meaning
bo	Extracting/starting firmware (boot)
01	The device is in normal operating mode and tries to obtain network parameters from a BootP/DHCP server using DHCP requests
03	Downloading firmware via TFTP
04	Loading firmware in the Flash memory that was loaded via the network
05	The recently loaded firmware was successfully saved in the Flash memory
06	New firmware was successfully saved in the Flash memory, a rollout script was downloaded via TFTP and executed
08	The device is in Rescue mode and tries to obtain network parameters from a BootP/DHCP server using DHCP requests in order to request a firmware image
_ _ _	Initializing firmware
- - -	Firmware running in normal mode
rB	Device rebooting
0r	Recovery procedure is deactivated according to the installed customized default profile
0d	Customized default profile cannot be applied (e.g., it is not installed)

Messages during operation with the memory module:

Display	Meaning
5c	Save configuration data on the MEM PLUG
EC	Equal configuration - the configurations on the MEM PLUG and the device are the same
dC	Different configuration - the configurations on the MEM PLUG and the device are different
0C	The MEM PLUG is empty
FC	Not enough memory on the memory module to save the configuration
HC	This MEM PLUG is not compatible with the device, e.g., a wireless ID plug or an MRP master

Messages in Smart mode:

For Smart Mode, see “Restart, recovery procedure, and flashing the firmware” on page 191

Display	Meaning
51	Smart mode “No changes”
55	Smart mode “Recovery procedure”
56	Smart mode “Flash procedure”
57	Smart mode “Customized default profile”

In the event of an error:

Display	Meaning	Remedy
41	RAM test error	– Perform a voltage reset
42	Flash test error	– Perform a voltage reset
07	Error when executing the rollout script	– Check the rollout script for errors
17	Firmware transfer via TFTP or Xmodem failed (display changes from “03” to “17”)	– Check the physical connection. – Establish a point-to-point connection. – Make sure that the file (with the specified file name) exists and is in the correct directory. – Check the IP address of the TFTP server. – Activate the TFTP server. – Repeat the download.
19	File transfer was completed successfully, but the file is not a valid firmware version for the device	– Provide a valid firmware version with the previously specified file name. – Repeat the download.
30	Device temperature too high or too low	– The device has left the temperature range set in the web interface.
49	SFP module not supported or faulty	– Replace the SFP module with a supported and/or fully functional SFP module
HC	This MEM PLUG is not compatible with the device, e.g., a wireless ID plug or an MRP master	– Use a suitable MEM PLUG

The points under “Remedy” are recommendations; they do not all have to be carried out for every error.

For all other message codes that are not listed here, please contact Phoenix Contact.

9.2 Startup

9.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  -20°C to 60°C
– Maximum humidity, non-condensing:
  95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

9.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– The device
– Package slip
– Terminal block for the power supply connection (inserted)
– Terminal block for the signal contact, button

9.3 Installation of FL MGUARD GT/GT

NOTE: The housing must not be opened.

NOTE: The shielding ground of the connected twisted pair cables is electrically connected to the front plate.

9.3.1 Mounting/removal

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting and connection is as follows:

- Pull out the terminal block from the bottom of the FL MGUARD GT/GT and wire the connections as required.
- Tighten the screws on the screw terminal blocks with at least 0.22 Nm.
  Wait to insert the terminal block base.
- Mount the FL MGUARD GT/GT on a grounded 35 mm DIN rail according to DIN EN 60715.
  The device is grounded by snapping it onto a grounded DIN rail.

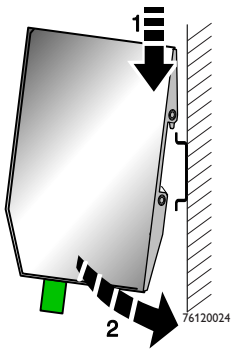


Figure 9-4 Mounting the FL MGUARD GT/GT on a DIN rail

- Attach the top snap-on foot of the FL MGUARD GT/GT to the DIN rail and then press the FL MGUARD GT/GT down towards the DIN rail until it engages with a click.
- Insert the required wired terminal blocks.
- Make any necessary network connections at the LAN port or WAN port (see “Connecting to the network” on page 178).
- Connect the corresponding device at the serial port as required (see “RS-232 interface for external management” on page 185).

Removal

- Remove or disconnect the connections.
- To remove the FL MGUARD GT/GT from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the FL MGUARD GT/GT.

9.3.2 Connecting to the network

The network can be connected with twisted pair cables via the RJ45 ports or via SFP slots with fiber optics.

The LAN or WAN RJ45 ports are disabled after the next reboot of the device if an SFP module is inserted in the corresponding slot.

9.3.2.1 RJ45 ports

The FL MGUARD GT/GT has two RJ45 ports, which support both 10/100 Mbps and 1000 Mbps and can be configured via the web interface.

NOTE: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

When connecting to the network, use cables with bend protection on the plugs.

LAN port

- Connect the local computer or the local network to the LAN port of the device using a UTP Ethernet cable (≥ **CAT5**) or using SFP plug-in modules (see “SFP slots” on page 180).

  If your computer is already connected to a network, patch the FL MGUARD GT/GT between the existing network connection.

Please note that configuration can only be completed via the LAN interface and that the firewall of the FL MGUARD GT/GT blocks all IP data traffic from the WAN to the LAN interface.

WAN port

- Use a UTP cable (≥ **CAT5**) or establish the connection using SFP plug-in modules (see “SFP slots” on page 180).
- Connect the external network via the WAN socket, e.g., WAN, Internet. (Connections to the remote device or network are established via this network.)

Driver installation is not required.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

Assignment of the RJ45 Ethernet plugs

Please note that for operation with 1000 Mbps (Gigabit), cables with four twisted pairs (eight wires), which meet the requirements of **CAT5e** as a minimum, must be used.

Table 9-3 Pin assignment of RJ45 plugs

Pin	10Base-T/10 Mbps	100Base-T/100 Mbps	1000Base-T/1000 Mbps
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_DC+ (bidirectional)
5	–	–	BI_DC- (bidirectional)
6	RD- (receive)	RD- (receive)	BI_DB- (bidirectional)
7	–	–	BI_DD+ (bidirectional)
8	–	–	BI_DD- (bidirectional)

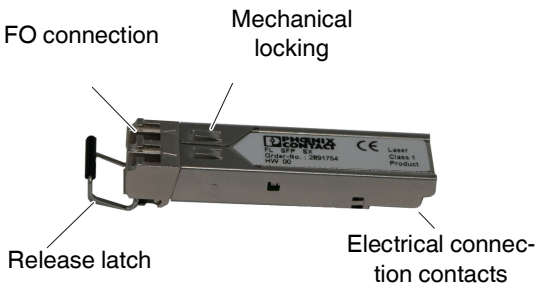
SFP slots

Inserted SFP modules are detected automatically when the device is switched on and the corresponding RJ45 port is disabled. Configuration of the SFP modules is not required because the modules are configured automatically (as of firmware 8.1.x).

The device supports both SFP modules with 100 and 1000 Mbps. Reboot the device when you change the speed of the used SPFs.

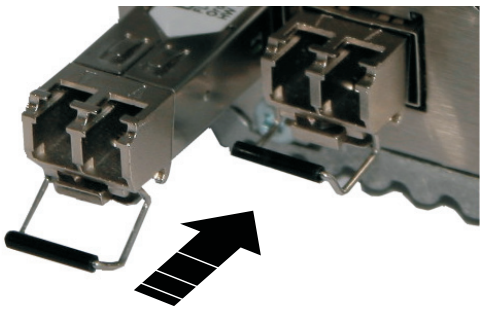
Use of the following SFP modules is recommended:

– FL SFP SX, 2891754
– FL SFP LX, 2891767
– FL SFP LH, 2989912
– FL SFP FX, 2891081
– FL SFP FX SM, 2891082



Elements of the SFP modules

The SFP slots are used by SFP modules (FO fiberglass modules in SFP format). By selecting the SFP modules, the user can specify whether the switch has multi-mode or single-mode fiber optic ports, for example.

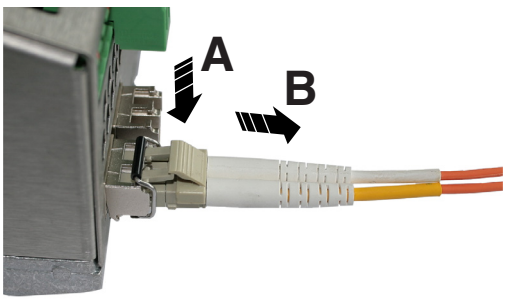


Inserting the SFP modules

- Insert the SFP modules in the relevant slots.
- Ensure correct mechanical alignment of the SFP modules.

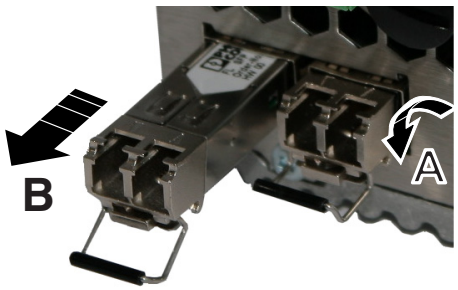
Connecting the FO cable

- Ensure correct mechanical alignment when inserting the fiber optic plugs.



Removing the fiber optic plugs

- Press the arresting latch (A) and pull out the plug (B).



Removing the SFP modules

- Remove the fiber optic plug before removing the SFP module.
- Turn the release latch (A) down and pull out the SFP module (B).

9.3.3 Connecting service contacts

Signal contact

WARNING: Only SELV circuits with voltage limitations according to EN 60950-1 may be connected to the signal contact.

The signal contact monitors the FL MGUARD GT/GT and thus enables remote diagnostics. Interruption of the contact via the floating signal contact (relay contact, closed current circuit) indicates the following:

– Failure of at least one of the two supply voltages.
– Power supply of the FL MGUARD GT/GT below the specified limit value (supply voltage 1 and/or 2 is less than 18 V).
– The faulty link status of at least one port. The link status message for each port can be masked on the FL MGUARD GT/GT via the management software.
  By default upon delivery, there is no connection monitoring.
– Error during selftest.

During a restart, the signal contact is interrupted until the device has started up completely. This also applies when the signal contact is manually set to “Closed” in the software configuration.

The switch has a floating signal contact. An error is indicated when the contact is opened.

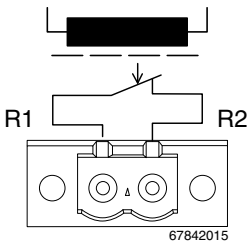


Figure 9-5 Basic circuit diagram for the signal contact

Enable contact (VPN / firewall rule record)

Always supply the enable button from the voltage source that supplies the FL MGUARD GT/GT VPN.

A **button** or an **on/off switch** (e.g., key switch) can be connected to enable contacts **MC1**.

The **button** or **on/off switch** is used to establish and release configured VPN connections or to activate configured firewall rule records.

Operating a connected button

- To establish VPN connections or to activate firewall rule records, hold down the button for a few seconds.
- To release VPN connections or to activate firewall rule records, hold down the button for a few seconds.

Operating a connected on/off switch

- To establish VPN connections or to activate firewall rule records, set the switch to the ON position.
- To release VPN connections or to activate firewall rule records, set the switch to the OFF position.

INF LED

If the INF LED does not light up, this generally indicates that the defined VPN connection is not present. Either the VPN connection was not established or it has failed due to an error.

If the INF LED is illuminated, the VPN connection is present.

If the INF LED is flashing, the VPN connection is being established or released.

9.3.4 Service contacts as of firmware version 8.1

Input/MC1

Via the web interface under “Management >> Service I/O”, you can set whether a push button or an on/off switch has been connected to the inputs. One or more freely selectable VPN connections or firewall rule records can be switched via the corresponding switch.

The web interface displays which VPN connections and which firewall rule records are connected to this input.

The push button or on/off switch is used to establish and release predefined VPN connections or the defined firewall rule records.

Operating a connected push button

- To switch on the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.
- To switch off the selected VPN connections or firewall rule records, press and hold the push button for a few seconds and then release the push button.

Operating a connected on/off switch

- To switch on the selected VPN connections or firewall rule records, set the switch to ON.
- To switch off the selected VPN connections or firewall rule records, set the switch to OFF.

9.3.5 Connecting the supply voltage

The device is designed for operation with a DC voltage of 18 V DC ... 32 V DC/SELV, 0.5 A maximum.

Therefore, only SELV circuits with voltage limitations according to IEC 60950/EN 60950/VDE 0805 may be connected to the supply connections and the signal contact.

Please note that there are several options when connecting the supply voltage and the optional enable button/signal contact:

– Easy connection of the supply voltage
– **Redundant connection** of the supply voltage

FL MGUARD GT/GT - you can connect **an enable button** to the **MCI** connection terminal blocks.

The MC1/GND connection terminal blocks can be used either for the connection of a (redundant) power supply or an enable button.

Monitoring of the redundant supply voltage and use of the MC1 input cannot be performed simultaneously. In this case, deactivate the monitoring of the redundant power supply under “Management >> Service I/O >> Alarm Output“.

9.3.5.1 Easy connection of the supply voltage

Signal contact without enable button

The supply voltage is connected via a terminal block with screw locking, which is located under the front of the device.

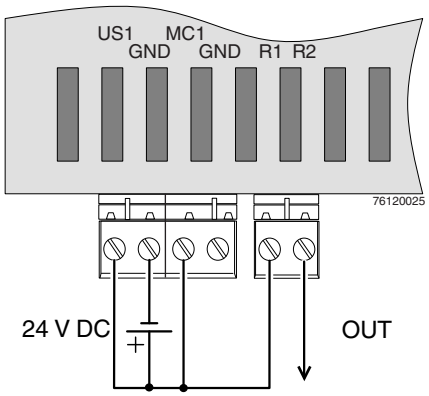


Figure 9-6 Easy connection of the supply voltage/signal contact without enable button

9.3.5.2 Redundant connection of the supply voltage

Signal contact without enable button

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the FL MGUARD GT/GT alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the FL MGUARD GT/GT indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs.

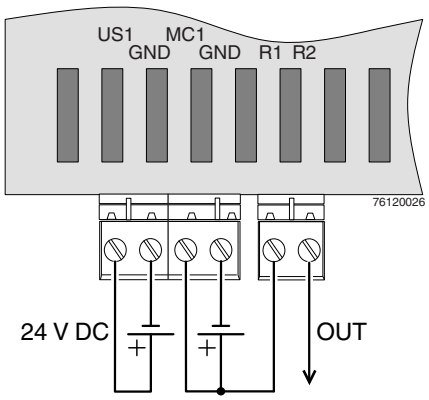


Figure 9-7 Redundant connection of the supply voltage/signal contact without enable button

9.3.5.3 Easy connection of the supply voltage with VPN enable button

Always supply the enable button/switch from the voltage source that supplies the FL MGUARD GT/GT VPN.

To enable a enable button/switch connected externally to the device to establish/release a VPN tunnel or to activate a firewall rule record, this button/switch should be connected to MC1.

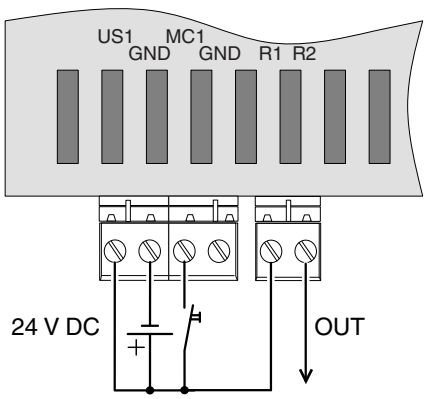


Figure 9-8 Easy connection of the supply voltage with enable button/switch

9.3.5.4 Redundant connection of the supply voltage with enable button/switch

NOTE: Only use power supplies that are suitable for parallel operation.

Always supply the enable contact from the voltage source that supplies the **FL MGUARD GT/GT**.

Monitoring of the redundant supply voltage and use of the MC1 input cannot be performed simultaneously. In this case, deactivate the monitoring of the redundant power supply under “Management >> Service I/O >> Alarm Output“.

To enable a VPN enable button/switch connected externally to the device to establish/release a VPN tunnel or to activate a firewall rule record, this switch/button should be connected to MC1.

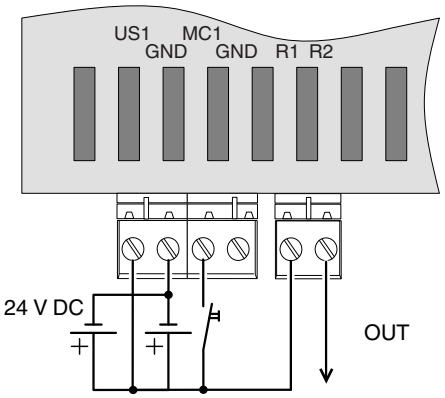


Figure 9-9 Redundant connection of the supply voltage with VPN enable button

9.3.6 RS-232 interface for external management

The 6-pos. Mini-DIN socket provides a serial interface to connect a local management station. It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface.

Set the following transmission parameters:

Bits per second	38,400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

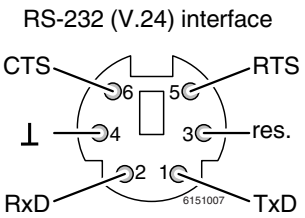


Figure 9-10 Transmission parameters and assignment of the RS-232 interface

9.4 Preparing the configuration

9.4.1 Connection requirements

- The **FL MGUARD GT/GT** must be connected to at least one active power supply unit.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
- **For remote configuration**: The device must be configured so that remote configuration is permitted.
- The device must be connected, i.e., the required connections must be working.

9.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following address:

Table 9-4 Preset addresses

Default setting	Network mode	Management IP address #1 (IP address of the internal interface)
FL MGUARD GT/GT	Router	https://192.168.1.1/

9.4.3 Configuration in Router mode

By default upon delivery, following reset to the default settings or after flashing the device, the device can be accessed within the network 192.168.1.0/24 via the LAN interface under IP address 192.168.1.1.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

9.5 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via one of the following addresses:

Table 9-5 Preset addresses

Default setting	Network mode	Management IP address #1 (IP address of the internal interface)
FL MGUARD GT/GT	Router	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 9-5).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure.

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 186).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.

  Click on “Properties” under “LAN settings”.

  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 9-11 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

9.6 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

9.7 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 38400
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

9.8 Restart, recovery procedure, and flashing the firmware

Smart mode enables the user to execute special functions without having to access the management interfaces.

The FL MGUARD GT/GT offers the following setting options via Smart mode:

– Performing a restart
– Performing a recovery procedure
– Perform flashing the firmware/rescue procedure

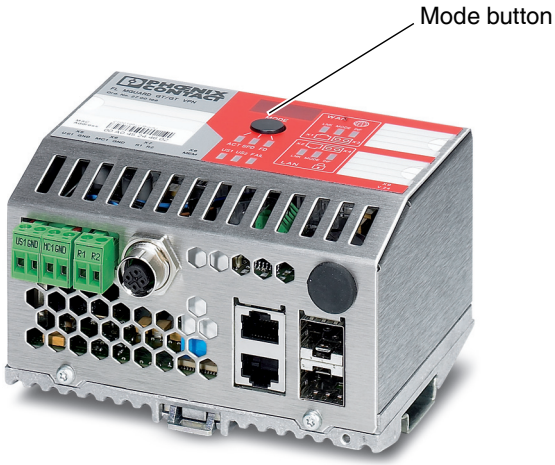


Figure 9-12 Mode button

9.8.1 Function selection by means of mode button (Smart mode)

Activating Smart mode

The Mode button is used to call/exit Smart mode and to select the desired function. The three mode LEDs indicate the mode that is currently set and the mode which will apply when exiting Smart mode.

Calling Smart mode

- Disconnect the device from the power supply.
- As soon as the supply voltage is switched on, hold down the Mode button for **more than ten seconds**. The three mode LEDs flash briefly three times and indicate that Smart mode is active.
- When Smart mode is started, the device is initially in the “Exit without changes” state (“51” in the display).

Selecting the desired setting

- To select the different settings, press the Mode button briefly and select the desired operating mode using a binary light pattern of the mode LEDs and a code on the 7-segment display.

Exiting Smart mode and activating the selection

- To exit, press and hold down the Mode button for at least five seconds. The previously selected function is executed.

Possible functions in Smart mode

The device supports the selection of the following functions in Smart mode (see also example below):

Table 9-6 Functions in Smart mode

Function	7-segment display	ACT LED 1	SPD LED 2	FD LED 3
Exit Smart mode without changes	51	Off	Off	**On**
Activate the recovery procedure	55	**On**	Off	**On**
Activate the flash procedure	56	**On**	**On**	Off
Apply customized default profile	57	**On**	**On**	**On**

9.8.2 Performing a restart

Objective

The device is restarted with the configured settings.

Action

See "Function selection by means of mode button (Smart mode)" for how to start the function type.
(Alternatively, disconnect the power supply and then connect it again.)

9.8.3 Performing a recovery procedure

Objective (to 8.3.x)

To mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

Use the recovery procedure if you do not know the IP address under which the device can be accessed.

The following network setting is restored:

Table 9-7 Restored network setting

Network Mode	Management IP #1 (IP address for internal interface)
Router	https://192.168.1.1/

The device is reset to router mode with the fixed IP address.

– The CIFS integrity monitoring function is also disabled because this only works in Stealth mode when the management IP is active.
– In addition, MAU configuration is activated for the Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The configured IP address of the device differs from the default setting.

– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (from 8.4.0)

From mGuard firmware version 8.4.0

The total configuration (not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration is automatically saved on the device and can be restored after a successful recovery procedure.

The following network setting is restored:

Table 9-8 Restored network setting

Network Mode	Management IP #1 (IP address for internal interface)
Router	https://192.168.1.1/

Recovery procedure steps from mGuard firmware version 8.4.0

Before performing the recovery procedure, the current device configuration is stored in a newly created configuration profile (“Recovery DATE”). Following the recovery procedure, the device starts with the default settings.

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.

Action

See "Function selection by means of mode button (Smart mode)" for how to start the function type.

If successful, the device restarts after two seconds and switches to Router mode. The device can then be reached again under the corresponding address (192.168.1.1).

From mGuard firmware version 8.4.0

- 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-2016.12.01-18:02:50").
- 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.

9.8.4 Perform flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

- **All configured settings are deleted.** The device is set to the delivery state.
- As of mGuard firmware version 5.0.0, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Prerequisites

NOTE: To flash the firmware, a DHCP and TFTP server or a BootP and TFTP server must be installed on the locally connected computer.

Install the DHCP and TFTP server, if necessary (see “Installing the DHCP and TFTP server” on page 195).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

Action

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure! Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

See "Function selection by means of mode button (Smart mode)" for how to start the function type (Smart Mode 56).

The status is displayed via the 7-segment display (see “Messages in the 7-segment display” on page 174).

Upon success, the device launches the rescue system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

The install.mpc83xx.p7s file is loaded from the TFTP server. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.

The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.

The jffs2.img.mpc83xx.p7s firmware file is downloaded from the TFTP server and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.

The process takes several minutes, during which the numbers on the 7-segment display change constantly. If **05** is shown in the display, the flash process has been concluded.

Subsequently, restart the device.The device is in the delivery state. Reconfigure the mGuard device (see “Establishing a local configuration connection” on page 188).

9.8.5 Installing the DHCP and TFTP server

Installing a second DHCP server in a network could affect the configuration of the entire network.

Under Windows

Install the program provided in the download area at phoenixcontact.net/products.

- If the Windows computer is connected to a network, disconnect it from the network.
- Copy the firmware to an empty folder on the Windows computer.
- 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.

- Click on **Browse** to switch to the folder where the mGuard image files are saved: **install.mpc83xx.p7s, jffs2.img.mpc83xx.p7s**
- If a major release upgrade of the firmware is carried out by flashing, the license file purchased for the upgrade must also be stored here under the name **licence.lic**.

  Make sure that this is the correct license file for the device (under “Management >> Update” on the web interface).

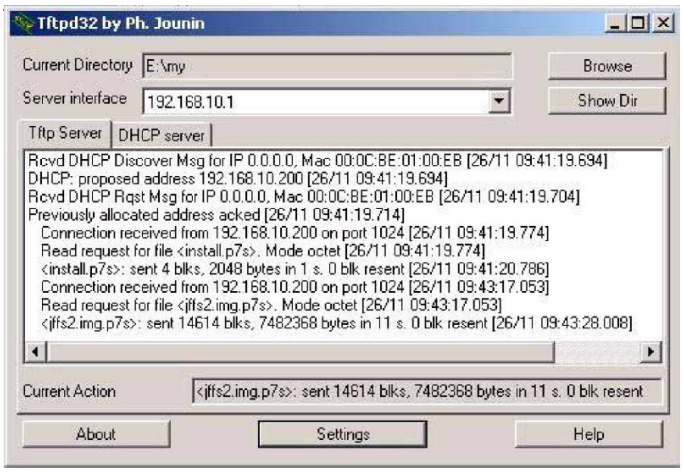
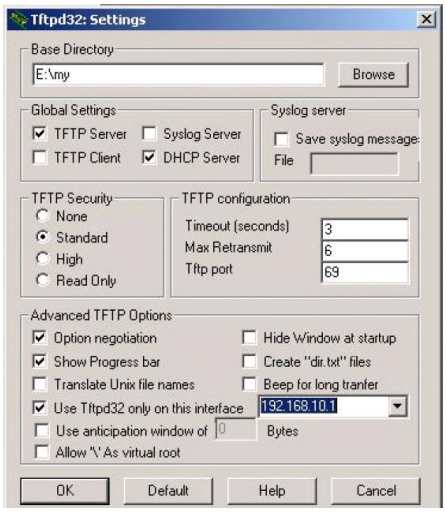


Figure 9-13 Entering the host IP

- Switch to the “TFTP Server” or “DHCP Server” tab page and click on “Settings” to set the parameters as follows:



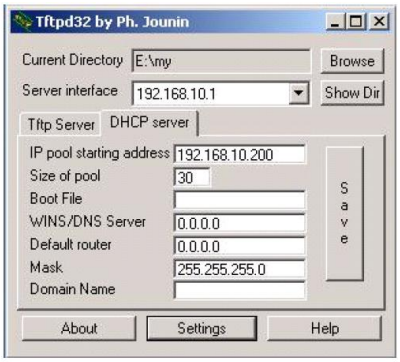


Figure 9-14 Settings

Under Linux

All current Linux distributions include DHCP and TFTP servers.

- Install the corresponding packages according to the instructions provided for the relevant distribution.
- 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**

- 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:
install.mpc83xx.p7s, jffs2.img.mpc83xx.p7s

- If a major release upgrade of the firmware is carried out by flashing, the license file purchased for the upgrade must also be stored here under the name **licence.lic**.

  Make sure that this is the correct license file for the device (under “Management >> Update” on the web interface).
- Then restart the inetd process to apply the configuration changes.
- If a different mechanism should be used, e.g., xinetd, please consult the relevant documentation.

9.9 Technical data

General data	FL MGUARD GT/GT
Function	Security applicance, firewall, routing, 1:1 NAT; VPN (optional), conforms to standard IEEE 802.3/802.3u/802.3ab
Firewall principle	Stateful inspection
SNMP	Version 2c, 3
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: max. 350 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 120 Mbps
Hardware-based encryption	DES | 3DES | AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: max. 110 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 60 Mbps
Management support	Web GUI (HTTPS) | command line interface (SSH) | SNMP v1/2/3 |central device management software | optional key switch (VPN)
Housing dimensions (width x height x depth) in mm	128 x 110 x 69 (depth from top edge of DIN rail) 128 x 150 x 69 (depth from top edge of DIN rail) with FL MEM PLUG (accessories)
Permissible operating temperature	-20°C ... 60°C
Permissible storage temperature	-40°C ... +85°C
Degree of protection	IP20, IEC 60529
Protection class	Class 3 VDE 0106; IEC 60536
Humidity	
Operation	5% ... 95%, non-condensing
Storage	5% ... 95%, non-condensing
Air pressure	
Operation	86 kPa ... 108 kPa, 1500 m above sea level
Storage	66 kPa ... 108 kPa, 3500 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Mounting position	Perpendicular to a standard DIN rail
Connection to protective earth ground	By snapping onto a grounded DIN rail
Weight	660 g, typical

Supply voltage (US1/US2 redundant)	FL MGUARD GT/GT
Connection	Via plug-in screw terminal block; max. conductor cross section = 2.5 mm^2
Nominal value	24 V DC
Permissible voltage range	18.0 V DC to 32.0 V DC
Permissible ripple (within the permissible voltage range)	3.6 V_{PP}
Test voltage	500 V DC for one minute
Current consumption on US at 24 V DC, maximum	270 mA
Maximum power consumption at nominal voltage	6.5 W

Interfaces	FL MGUARD GT/GT
Number of Ethernet ports	2, should be operated as RJ45 port or SFP port
RS-232 configuration interface	
Connection format	Mini-DIN socket

Interfaces [...]	FL MGUARD GT/GT
Floating signal contact	
Voltage	24 V DC
Current carrying capacity	100 mA

Ethernet interfaces	FL MGUARD GT/GT
Properties of RJ45 ports	
Quantity	2 with autocrossing and auto negotiation
Connection format	8-pos. RJ45 socket on the switch
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
Maximum network segment expansion	100 m
Properties of the SFP interfaces	
Quantity	2
Connection format	SFP slot module
Connection medium	Fiber optics
Connection	LC format
Data transmission speed	100 Mbps or 1000 Mbps (depending on SFP module used)
Maximum network expansion	Depending on the SFP module used
Optical fiber type	Depending on the SFP module used

Mechanical tests	FL MGUARD GT/GT
Shock testing according to IEC 60068-2-27	Operation: 30g/11 ms, Half-sine shock pulse Storage/transport: 50g, Half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage/transport: 5g, 57 Hz ... 150 Hz
Free fall according to IEC 60068-2-32	1 m

Conformance with EMC Directive 2004/108/EC and Low-Voltage Directive 2006/95/EC

Immunity test according to EN 61000-6-2[1]

				Test intensity
Electrostatic discharge (ESD)	EN 61000-4-2	Criterion B[2]	Contact discharge	2
			Air discharge	2
			Indirect discharge	3
Electromagnetic HF field	EN 61000-4-3	Criterion A[3]		3
Fast transients (burst)	EN 61000-4-4	Criterion B[2]	Data cables	2
			Voltage supply	3
Surge current loads (surge)	EN 61000-4-5	Criterion B[2]	Data cables	2
			Voltage supply	1
Conducted interference	EN 61000-4-6	Criterion A[3]	Test intensity 3	

Noise emission test according to EN 61000-6-4

Noise emission of housing	EN 55011[4]	Class A[5]		
Noise emission	EN 55022	Class B[6]		

[1] EN 61000 corresponds to IEC 61000

[2] Criterion B: Temporary adverse effects on the operating behavior, which the device corrects automatically.

[3] Criterion A: Normal operating behavior within the specified limits.

[4] EN 55011 corresponds to CISPR11

[5] Class A: Industrial application, without special installation measures

[6] Class B: residential

Additional certification	FL MGUARD GT/GT
RoHS	EEE 2002/95/EC - WEEE 2002/96/EC

10 FL MGUARD PCI(E)4000

Table 10-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD PCI4000	2701274
FL MGUARD PCI4000 VPN	2701275
FL MGUARD PCIE4000	2701277
FL MGUARD PCIE4000	2701278

Product description

The **FL MGUARD PCI(E)4000** has the design of a PCI-compatible plug-in board. It is available in two versions:

– **FL MGUARD PCI4000 (VPN)** for devices or machines with PCI bus
– **FL MGUARD PCIE4000** for devices or machines with PCI Express bus

To aid understanding, FL MGUARD PCI4000 is used for the two device versions in this user manual.

The FL MGUARD PCI4000 is suitable for distributed protection of industrial and panel PCs, individual machines or industrial robots. It has a configuration memory in the form of a replaceable SD card, which can be easily accessed on the front.

Figure 10-1 FL MGUARD PCI4000

10.1 Operating elements and LEDs

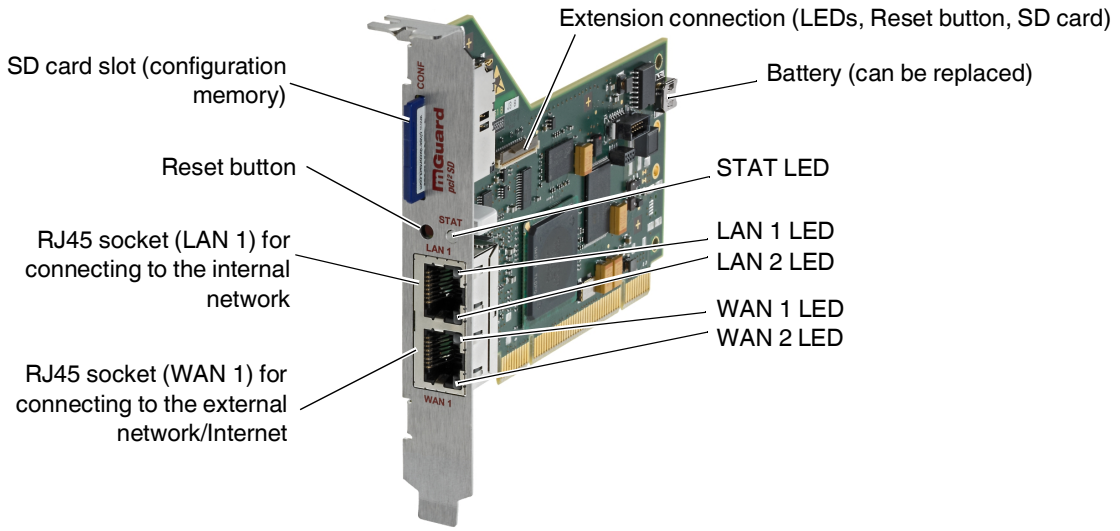


Figure 10-2 Operating elements and LEDs on the FL MGUARD PCI4000

Table 10-2 LEDs on the FL MGUARD PCI4000

LEDs	State		Meaning
WAN 1 **LAN 1**	Green	On	Full duplex
		Off	Half duplex
WAN 2 **LAN 2**	Yellow	On	10 Mbps
		Flash-ing	10 Mbps, data transmission active
	Green	On	100 Mbps
		Flash-ing	100 Mbps, data transmission active
LAN 1 **LAN 2** **WAN 1**	Various LED light codes		**Recovery procedure/flashing** See “Restart, recovery procedure, and flashing the firmware” on page 214.
STAT	Red/green	Flash-ing	**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	Flash-ing	**Heartbeat**. The device is connected correctly and ready to operate.
	Red	Flash-ing	**System error**. Restart the device. • Press the Reset button (for 1.5 seconds). • Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see “Performing a recovery procedure” on page 215) or contact your dealer.

10.2 Startup

10.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Connection notes

– A free PCI slot (3.3 V or 5 V) must be available on your PC when using the FL MGUARD PCI4000.
– Do not bend connecting cables. Only use the network plug for connection to a network.

NOTE: Select suitable ambient conditions

– Ambient temperature:
  0°C ... +60°C (FL MGUARD PCI4000 with battery)
  0°C ... +70°C (FL MGUARD PCI4000 without battery)
– Maximum humidity, non-condensing:
  5% ... 95%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

10.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– FL MGUARD PCI4000
– Package slip

10.3 Installation of FL MGUARD PCI4000

WARNING: 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.

WARNING: 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.

10.3.1 Installing the hardware

NOTE: Electrostatic discharge

Before installation, touch the metal frame of the PC in which the FL MGUARD PCI4000 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 61340-5-1.

FL MGUARD PCI4000: structure

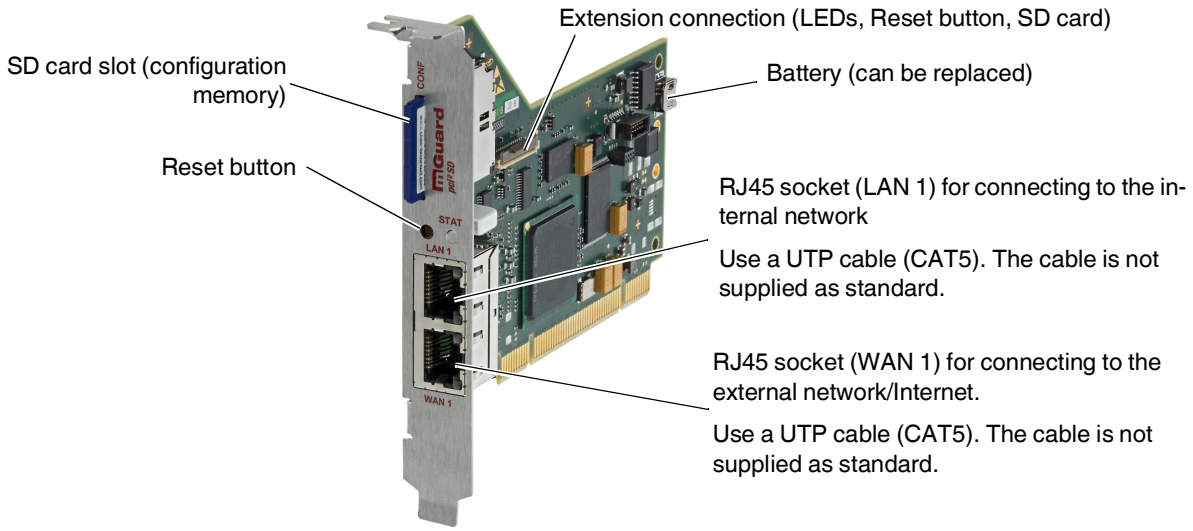


Figure 10-3 FL MGUARD PCI4000 structure

- Install the FL MGUARD PCI4000 in a free PCI or PCI Express slot. Observe the notes in the documentation for your system.

10.4 Preparing the configuration

10.4.1 Connection requirements

- **For local configuration**: The computer used for configuration must meet the following requirements:
  - The computer must be connected to the device LAN connection or to the device via the local network.
- **For remote configuration**: The device must be configured so that remote configuration is permitted.
- The device must be connected, i.e., the required connections must be working.

10.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following addresses:

Table 10-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 211). Alternatively, you can select a different stealth configuration or use another network mode.

10.5 Configuration in Stealth mode

The FL MGUARD PCI4000 can be started up in three different ways:

– Start up the device in Stealth mode (standard)
– Start up the device via temporary management IP address
– Start up device via BootP

10.5.1 Start up the device in Stealth mode (standard)

Insert the FL MGUARD PCI4000 between an existing network connection.

To connect to the LAN and WAN interfaces, a suitable UTP cable (CAT5) is required. The cables are not supplied as standard.

- Connect the internal network interface (LAN 1) of the FL MGUARD PCI4000 to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network.
- Connect the external network interface (WAN 1) of the FL MGUARD PCI4000 to the external network, e.g., Internet.

The STAT status LED lights up green when the supply voltage has been connected properly.

The device boots the firmware. The STAT status LED flashes green during this time.

The device is ready for operation as soon as the lower Ethernet socket LEDs light up. In addition, the STAT status LED flashes green at heartbeat.

If the lower LEDs in the Ethernet sockets do not light up, this indicates a missing connection to the internal or external network. If no LED lights up, the supply voltage is missing.

The device is configured via a web browser that is executed on the locally connected computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device is preset and can be accessed via address https://1.1.1.1/

Configuring the FL MGUARD PCI4000

- Enter the following address into the browser: https://1.1.1.1/

The connection to the FL MGUARD PCI4000 is established. (If not, see Section 10.5.2).

A security message indicating a possible invalid/not trusted certificate is displayed. This message results from the use of an mGuard certificate from Phoenix Contact that is not yet known to the browser but necessary for encryption of the communication.

- Acknowledge this message with “Accept this certificate always/temporarily” (Mozilla Firefox), “Continue loading this website” (Internet Explorer), “Continue anyway” (Google Chrome).
- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 10-4 Login

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

User Name:	admin
Password:	mGuard

To configure the device, make the desired or necessary settings on the individual pages of the mGuard web interface.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration (in the web interface under “Authentication >> Administrative Users”).

10.5.2 Starting up the FL MGUARD PCI4000 via a temporary management IP address

If the FL MGUARD PCI4000 is connected without a functioning external network in initial startup mode, the device **cannot** be accessed via address https://1.1.1.1/.

In this case, the FL MGUARD PCI4000 is accessible automatically via management IP address 192.168.1.1/24. This applies to the internal (LAN 1) and the external (WAN 1) network interfaces. An address conflict with the external network interface is not possible as long as WAN 1 is not connected to a functioning network. This management IP address is normally non-persistent.

However, if the external network interface (WAN 1) is connected after booting the FL MGUARD PCI4000, the management IP address remains valid. In this case, an address conflict with an existing address in the external network is possible.

Starting up the FL MGUARD PCI4000 without external network

- Connect the internal network interface (LAN 1) of the FL MGUARD PCI4000 to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network.
- Disconnect the external network interface (WAN 1) of the FL MGUARD PCI4000 from the external network (WAN).
- Switch on the system. The STAT LED lights up green when the supply voltage has been connected properly.

The device boots the firmware. The STAT LED flashes green.

Adapting the configuration computer

In order to access the FL MGUARD PCI4000 for configuration, the configuration computer must be adapted to the management IP address of the FL MGUARD PCI4000.

Example of Microsoft Windows XP:

- Set the following in the “Internet Protocol (TCP/IP) Properties” of the relevant network interface of the configuration computer:

IP address:	192.168.1.10
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.2

- Enter the address assigned into the browser: https://192.168.1.1/
- Configure the device as described in “Configuring the FL MGUARD PCI4000” on page 207.

10.5.3 Starting up FL MGUARD PCI4000 via BootP

In initial startup mode, the FL MGUARD PCI4000 additionally starts a BootP client on the internal network interface (LAN 1). The BootP client is compatible with the “IPAssign” BootP servers from Phoenix Contact as well as “DHCPD” under Linux.

This software can be downloaded free of charge at phoenixcontact.net/products.

IP address assignment using IPAssign is described in detail in “Assigning the IP address using IPAssign.exe” on page 273.

If an non-configured FL MGUARD PCI4000 accesses a BootP server after booting, the BootP protocol assigns an IP address, a subnet mask, and optionally a default gateway of the internal network interface to the FL MGUARD PCI4000. These parameters are saved in the device which can then be immediately accessed under these parameters.

- Enter the address assigned via BootP in the browser: e.g., https://192.168.1.1/

Configure the device as described in “Configuring the FL MGUARD PCI4000” on page 207.

10.5.4 Assigning the IP address via BootP

After assigning an IP address via BootP, the product can no longer be accessed via IP address 192.168.1.1

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

Section 14.1 explains IP address assignment using the free Windows software "IP Assignment Tool" (IPAssign.exe).

Notes for BootP

During initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the device no longer sends BootP requests. The product 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) must be performed.

10.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via the following address:

Table 10-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 10-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 215).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 205).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.
  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.
  Click on “Properties” under “LAN settings”.
  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.
  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 10-5 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

10.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

10.8 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

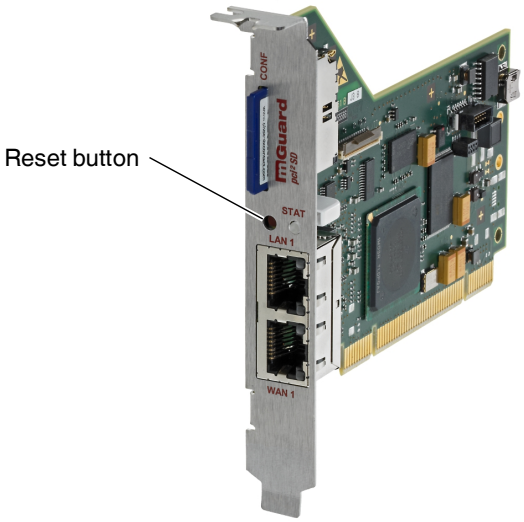


Figure 10-6 Reset button

10.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button until the STAT LED lights up orange.
- Alternatively, restart the computer that contains the FL MGUARD PCI card.

10.8.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

When performing the recovery procedure, the default network settings are established:

Table 10-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is reset to Stealth mode with the default setting “multiple Clients”.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The configured IP address of the device differs from the default setting.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 10-6 Preset addresses

Default setting	Networ k mode	Management IP #1	Management IP #2
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately 2 seconds, the STAT LED lights up green.
- Press the Reset button slowly again six times.
  If successful, the STAT LED lights up green.
  If unsuccessful, the STAT LED lights up red.

If successful, the device restarts after two seconds and switches to Stealth mode. The device can then be reached again under the corresponding addresses.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

10.8.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

– **All configured settings are deleted.** The device is set to the delivery state.
– In mGuard firmware version 5.0.0 or later, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

– All necessary firmware files must be located in a common directory on the first partition of the SD card.
– This partition must use a VFAT file system (standard type for SD cards).

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

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

The following requirements apply when loading the firmware from an SD card:

– All necessary firmware files must be located in a common directory on the first partition of the SD card.
– This partition must use a VFAT file system (standard type for SD cards).
– The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.
– This SD card has been inserted into the device.
– The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:
  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s

Action

- Press and hold down the Reset button on the front plate.
  The STAT LED on the front plate briefly lights up orange.
  Then the STAT LED and the LEDs of the Ethernet sockets (LAN1, LAN2, WAN1) light up green one after the other.
- Release the Reset button during the green light phase.
  The flashing procedure is started.

10.9 Technical data

Hardware properties		FL MGUARD PCI4000 I FL MGUARD PCIE4000
Platform		Freescale network processor with 330 MHz clocking
Network interfaces		1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ45 I full duplex I auto MDIX
Other interfaces		Serial RS-232, internal connector
Memory		128 MB RAM I 128 MB Flash SD card I replaceable configuration memory
Drives		–
Redundancy options		Optional: VPN I router
Power supply		3.3 V or 5 V via PCI (FL MGUARD PCI4000) or PCI Express bus (FL MGUARD PCIE4000)
Power consumption		Typical, 3.7 W ... 4.2 W
Humidity range		5% ... 95% during operation and storage, non-condensing
Degree of protection		Depending on installation type and on the host system
Temperature range	Without battery (HT version)	0°C ... +70°C (operation) -20°C ... +70°C (storage)
	With battery	0°C ... +60°C (operation) -20°C ... +60°C (storage)
Dimensions (H x W x D)		95 mm X 18 mm X 130 mm
Weight		131 g
Weight (incl. packaging)		200 g

Firmware and power values	FL MGUARD PCI4000 I FL MGUARD PCIE4000
Firmware compatibility	For mGuard v7.5.0 or later: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: max. 120 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 50 Mbps
Hardware-based encryption	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: max. 30 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 20 Mbps
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (2 x LAN, 2 x WAN in combination) for Ethernet status and speed; 1 LED for Power, Error, State, Fault, Info) I log file I remote-syslog

Other	FL MGUARD PCI4000 I FL MGUARD PCIE4000
Conformance	CE I FCC
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Remote Services Portal ready

11 FL MGUARD SMART2

Table 11-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD SMART2	2700640
FL MGUARD SMART2 VPN	2700639

Product description

The **FL MGUARD SMART2** is the smallest device version. For example, it can be inserted between the computer or local network and an available router, without having to make configuration changes or perform driver installations on the existing system. It is designed for instant use in the office or when traveling.

Figure 11-1 FL MGUARD SMART2

11.1 Operating elements and LEDs

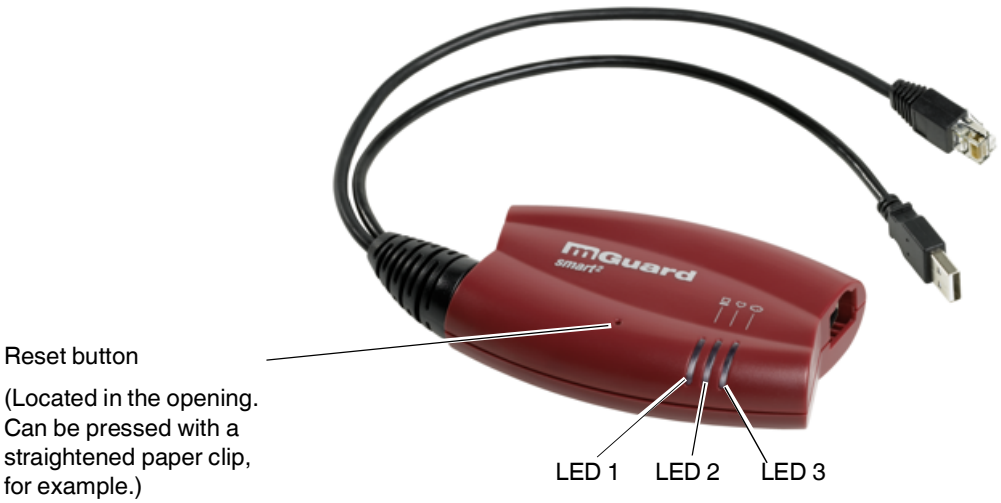


Figure 11-2 Operating elements and LEDs on the FL MGUARD SMART2

Table 11-2 LEDs on the FL MGUARD SMART2

LED	State		Meaning
1	Green	On	LAN: connection to the network partner is present
		Flashing	LAN: data transmission is active
2	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 correctly connected and operating.
	Red	Flashing	**System error**. Restart the device. • Press the Reset button (for 1.5 seconds). • Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see “Performing a recovery procedure” on page 231) or contact your dealer.
3	Green	On	WAN: connection to the network partner is present
		Flashing	WAN: data transmission is active
1, 2, 3	Various LED light codes		**Recovery mode**. After pressing the **Reset button**. See “Restart, recovery procedure, and flashing the firmware” on page 230.

11.2 Startup

11.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  0°C ... +40°C
– Maximum humidity, non-condensing
  20% ... 90%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

11.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– FL MGUARD SMART2
– Package slip

11.3 Connecting the FL MGUARD SMART2

LAN port

Ethernet plug for direct connection to the device or network to be protected (**local** device or network).

USB plug

For connection to the USB interface of a computer.

For the power supply (default settings).

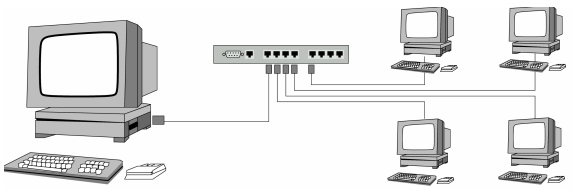
The FL MGUARD SMART2 (not the FL MGUARD SMART) can be configured so that a serial console is available via the USB plug.

WAN port

Socket for connection to the external network, e.g., WAN, Internet. (Connections to the remote device or network are established via this network.)

Use a UTP cable (CAT5).

Before:



After:

(A LAN can also be on the left.)

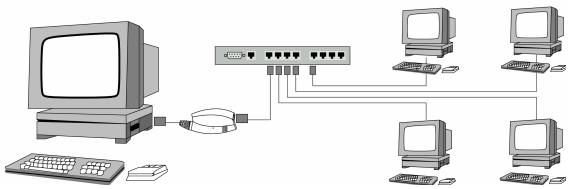


Figure 11-3 FL MGUARD SMART2: Connection in the network

If your computer is already connected to a network, insert the FL MGUARD SMART2 between the network interface of the computer (i.e., its network card) and the network.

Driver installation is not required.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

WARNING: 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.

11.4 Preparing the configuration

11.4.1 Connection requirements

- The FL MGUARD SMART2 must be switched on, i.e., it must be connected to a computer (or power supply unit) that is switched on via a USB cable in order for it to be supplied with power.
- **For local configuration**: The computer used for configuration:
  - Must be connected to the LAN port of the device
  - Or must be connected to the device via the local network
- **For remote configuration**: The device must be configured so that remote configuration is permitted.
- The device must be connected, i.e., the required connections must be working.

11.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following addresses:

Table 11-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 227). Alternatively, you can select a different stealth configuration or use another network mode.

11.5 Configuration in Stealth mode

On initial startup, the device can be accessed via two addresses:

– https://192.168.1.1/ (see Page 225)
– https://1.1.1.1/ (see Page 225)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 226).

The device can be accessed via https://192.168.1.1/ if the external network interface is not connected on startup.

Computers can access the device via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the device. For this purpose, the device with LAN port and WAN port must be integrated in an operational network in which the default gateway can be accessed via the WAN port.

– After access via IP address 192.168.1.1 and successful login, IP address 192.168.1.1 is set as a fixed management IP address.
– After access via IP address 1.1.1.1 or after IP address assignment via BootP, the product can no longer be accessed via IP address 192.168.1.1.

11.5.1 IP address 192.168.1.1

In Stealth mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.

– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

11.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the device to be addressed via address **https://1.1.1.1/,** it must be connected to a configured network interface. This is the case if it is connected in an existing network connection and if the default gateway can be accessed via the WAN port of the device at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 227). Continue from this point.

After access via IP address 1.1.1.1, the product can no longer be accessed via IP address 192.168.1.1

11.5.3 Assigning the IP address via BootP

After assigning an IP address via BootP, the product can no longer be accessed via IP address 192.168.1.1

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

Section 14.1 explains IP address assignment using the free Windows software "IP Assignment Tool" (IPAssign.exe).

Notes for BootP

During initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the device no longer sends BootP requests. The product 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) must be performed.

11.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via one of the following addresses:

Table 11-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network setting”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 11-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 231).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 223).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.
  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.
  Click on “Properties” under “LAN settings”.
  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.
  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 11-4 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

11.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

11.8 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

Reset button

(Located in the opening. Can be pressed with a straightened paper clip, for example.)

Figure 11-5 Reset button

11.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the middle LED lights up in red.
  (Alternatively, you can disconnect and insert the USB cable, as it is only used for the power supply.)

11.8.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

When performing the recovery procedure, the default network settings are established:

Table 11-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is reset to Stealth mode with the default setting “multiple Clients”.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The configured IP address of the device differs from the default setting.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 11-6 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately 2 seconds, the middle LED lights up green.
- Press the Reset button slowly again six times.
  If successful, the middle LED lights up green.
  If unsuccessful, the middle LED lights up red.

If successful, the device restarts after two seconds and switches to Stealth mode. The device can then be reached again under the corresponding addresses.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

11.8.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

– **All configured settings are deleted.** The device is set to the delivery state.
– In mGuard firmware version 5.0.0 or later, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

NOTE: To flash the firmware, a DHCP and TFTP server or a BootP and TFTP server must be installed on the locally connected computer.

Install the DHCP and TFTP server, if necessary (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

Action

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the LEDs light up green. Then, the device is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**
  If the Reset button is not released, the device is restarted.
  The device now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.
  The middle LED flashes.
  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.
  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.
  The three green LEDs form a running light.
  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.
  This process takes around 3 to 5 minutes. The middle LED is lit continuously.
  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.
- As soon as the procedure is complete, all LEDs flash green simultaneously.
- Restart the device. To do this, briefly press the **Reset button**.
  Alternatively, you can disconnect and insert the USB cable, as it is only used for the power supply.

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 227):

11.9 Technical data

Hardware properties	FL MGUARD SMART2
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ45 I full duplex I auto MDIX
Other interfaces	Serial via USB connection
Drives	–
Redundancy options	Depending on the firmware used
Power supply	Via USB interface (5 V at 500 mA) Optional: external power supply unit (110 V ... 230 V)
Power consumption	2.5 W, maximum
Temperature range	0°C ... +40°C (operation) -20°C ... +60°C (storage)
Humidity range	20% ... 90% during operation, non-condensing
Degree of protection	IP30
Dimensions (H x W x D)	27 x 77 x 115 mm
Weight	185 g

Firmware and power values	FL MGUARD SMART2
Firmware compatibility	For mGuard v7.2 or later: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: max. 120 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 50 Mbps
Hardware-based encryption	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: max. 30 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 20 Mbps
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	3 LEDs (in combination for boot process, heartbeat, system error, Ethernet status, Recovery mode) I Log File I Remote Syslog

Other	FL MGUARD SMART2
Conformance	CE I FCC
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor

12 FL MGUARD CENTERPORT

Table 12-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD CENTERPORT	2702547

Product description

The **FL MGUARD CENTERPORT** is a high-end firewall and a VPN gateway in 19" format. It is suitable as a central network infrastructure for remote service solutions. With its Gigabit Ethernet interfaces and corresponding throughput as the router and as the stateful inspection firewall, the device can also be used in the backbone in industrial networks.

As a gateway, the FL MGUARD CENTERPORT supports the VPN connection to any number of systems in the VPN tunnel groups with optionally up to three thousand simultaneously active tunnels, which all belong to the same unique public IP address.

The FL MGUARD CENTERPORT performs secure remote services, such as remote support, remote diagnostics, remote maintenance, and condition monitoring for a large number of machines and systems via the Internet. An encrypted VPN data throughput of 600 Mbps is possible at one interface.

The FL MGUARD CENTERPORT is compatible with all mGuard field devices and the MGUARD DM. VPN licenses can be installed later, if required.

Figure 12-1 FL MGUARD CENTERPORT

12.1 Operating elements and LEDs

Front

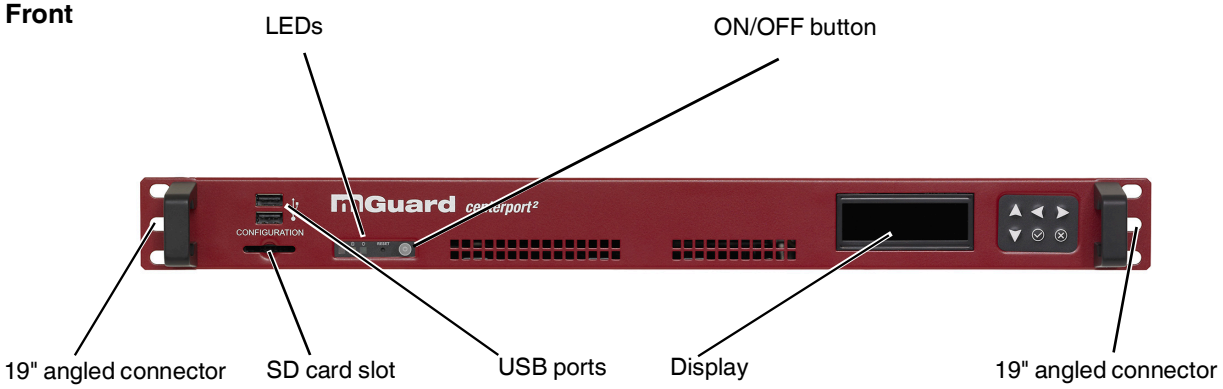


Figure 12-2 Operating elements and LEDs on the FL MGUARD CENTERPORT front side

Table 12-2 LEDs on the FL MGUARD CENTERPORT

LED	State	Meaning
Green	On	Lights up if the system is switched on
Orange	On	Lights up while hard disk is accessed

12.2 Startup

12.2.1 Safety notes

Personnel

Installation, startup and maintenance of the product may only be performed by qualified specialist personnel who have been authorized for this by the operator. Specialist personnel must have read and understood the instructions in this manual and act accordingly.

NOTE: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C ... +45°C
- Maximum humidity, non-condensing:
  20% ... 90%

To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Risk of material damage caused by cleaning agents

Clean the device housing with a soft cloth. Do not use aggressive solvents.

12.2.2 Checking the scope of supply

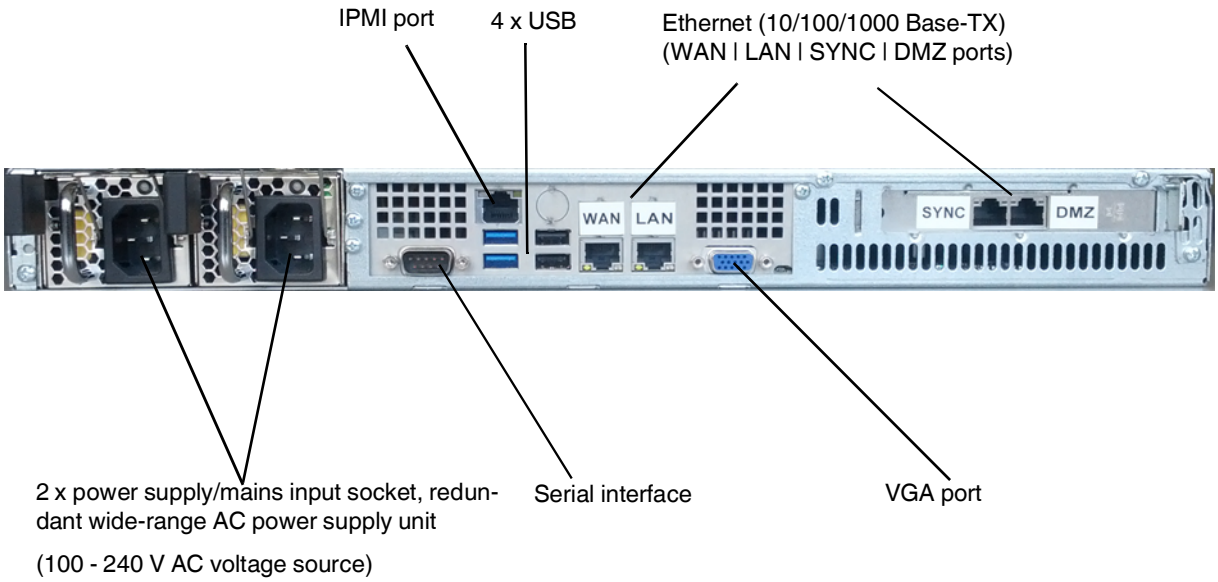
Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

- FL MGUARD CENTERPORT
- Package slip
- 2 x AC mains connecting cables
- 19" server rails/telescopic rails (2 x short, 2 x long)
- Screw set
- Installation instructions for 19" frame/industrial cabinet (Quickrails installation instructions)

12.3 Installing and booting the FL MGUARD CENTERPORT

Back (Model until 2022)



Back (Model from 2023)

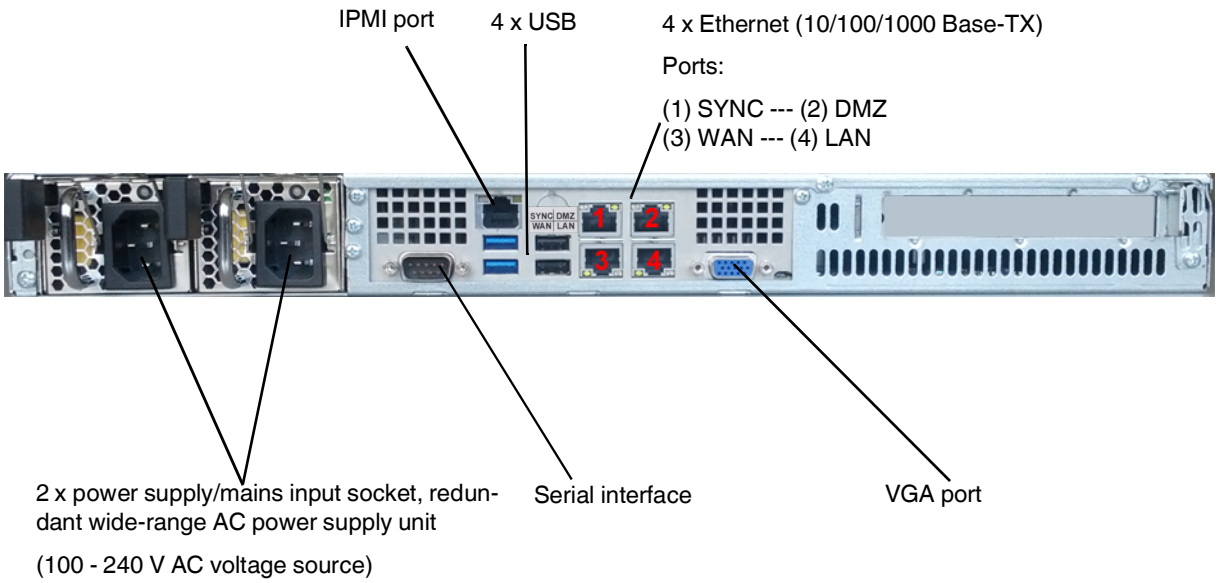


Figure 12-3 FL MGUARD CENTERPORT back

12.3.1 Connecting the device

2. Optional: Install the device in a 19" frame/industrial cabinet (“Installation in a 19" frame/industrial cabinet” on page 241).
3. Connect the two mains input sockets to the mains or power supply source (100 - 240 V AC) using a mains connecting cable.

To ensure that the status of the power supply (power supply 1/2) is displayed correctly in the WBM, the (redundant) power supply must already have been connected correctly before the device is switched on.

If this is not the case, you must shut down the device and disconnect the power supply completely from the device for at least 30 seconds. Then reconnect the power supply correctly to the device and restart it.

4. Connect the network connections (see “Connecting the network connections” on page 239).
5. Optional: Connect a PC monitor to the VGA port (not supplied as standard).
6. Optional: Connect a PC keyboard to one of the USB connections (not supplied as standard).

The keyboard and monitor do not need to be connected to start and operate the device. The monitor and keyboard must only be connected

- in order to use one of the boot options upon starting (booting) the device (see “Boot options - when monitor and keyboard are connected” on page 241).
- in order to perform a rescue procedure or recovery procedure. See “Restart, recovery procedure, and flashing the firmware” on page 247.

12.3.2 Connecting the network connections

WARNING: Only connect the device network ports to LAN installations.

Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

LAN port

- Use a UTP cable (CAT5).
- Connect the LAN port of the device to the corresponding Ethernet network card of the local configuration computer or a network connection of the local network (LAN).

WAN port

- Use a UTP cable (CAT5).
- Connect the WAN port of the device to the external network or the Internet. (Connections to the remote device or network are established via this network.)

SYNC port

- Use a UTP cable (CAT5).
- Connect the SYNC port of the device to the SYNC port of a second FL MGUARD CENTERPORT in order to create a redundancy pair. A redundancy license for the second FL MGUARD CENTERPORT must be purchased separately.

DMZ port

- Use a UTP cable (CAT5).
- Connect the DMZ port of the device to a network connection of the local network (LAN). This network is used for communication according to the firewall rules of the demilitarized zone (DMZ).

IPMI port

- Use a UTP cable (CAT5).

By default, the **IPMI port** is deactivated and not documented at this point. The IPMI port functions can be activated in the BIOS setup of the motherboard. Should you have any questions on the documentation, please contact Super Micro Computer, Inc. (http://www.supermicro.com).

Serial interface

NOTE: The serial interface (D-SUB socket) must not be connected directly to telecommunications connections. To connect a serial terminal or a modem, use a serial cable with D-SUB connector. The maximum cable length of the serial cable is 30 m.

The serial interface (serial port) can be used as follows:

To configure the device via the serial interface. There are two options:

– A PC is connected directly to the serial interface of the device (via the serial interface of the PC). The PC user can then use a terminal program to configure the device via the command line.

– Or a modem is connected to the serial interface of the device. This modem is connected to the telephone network (fixed-line or GSM network). The user of a remote PC, which is also connected to the telephone network via a modem, can then establish a PPP (Point-to Point Protocol) dial-up line connection to the device and configure it via a web browser.

To manage data traffic via the serial interface instead of via the WAN interface of the device. In this case, a modem should be connected to the serial interface.

12.3.3 Installation in a 19" frame/industrial cabinet

The mains connecting cables of the power supply units are used as mains disconnect points. Sockets that can easily be accessed and that are close to the device must therefore be used for the mains plug. Unplug the mains plug to disconnect the device from the mains. If the device is installed in a control cabinet where the sockets cannot be accessed, an adequate disconnecting device must be installed during installation (e.g., an approved disconnector).

Sufficient air circulation must be ensured. If several FL MGUARD CENTERPORT devices are stacked, one or 19" fan trays must be provided to discharge the accumulated warm air. The control cabinets used must conform to the requirements of fire-protection casings and mechanical protection according to EN 60950-1.

For information on installing the FL MGUARD CENTERPORT, please refer to the “Quickrails installation instructions” provided with the device.

12.3.4 Starting (booting) the FL MGUARD CENTERPORT

- Switch on the device by pressing the ON/OFF button.
- After switching on the device, the status LED lights up (green). Another LED (orange) lights up each time accessing the non-volatile memory.
- The device boots the firmware and is ready to operate.
- The display shows status messages of the mGuard firmware.

12.3.4.1 Boot options - when monitor and keyboard are connected

If a monitor and a keyboard are connected to the device, the following options are available:

– Following switch-on

– Following a restart

the boot messages from the BIOS are initially displayed on the monitor.

If the boot menu is to be displayed, press one of the direction keys several times: ↑, ↓, ← or →.

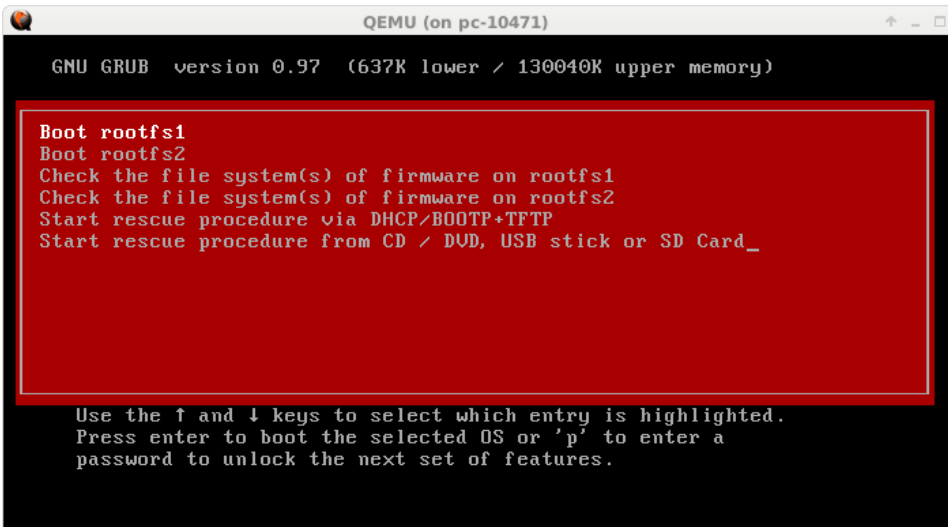


Figure 12-4 FL MGUARD CENTERPORT boot menu

To select and apply one of the boot options, proceed as follows:

1. Select one of the displayed options with the direction keys ↓ or ↑.
2. Then press the **Enter** button.

Boot options

Boot rootfs1

Start the primary firmware version on the device (A). This is the default setting: it is applied if the user does not intervene during startup.

Boot rootfs2

Not supported by the current firmware version.

Check the file system(s) of firmware on rootfs1

If required, checks and repairs all firmware file systems.
This menu item is only to be used in special cases when the user has the appropriate knowledge or upon instruction from the dealer support team. The mGuard firmware checks and repairs the file systems, if required, even during the normal startup process. The firmware uses its file systems in a highly robust manner when the mass storage device cache is switched off, so that there is not usually any need for repairs.

Check the file system(s) of firmware on rootfs2

Not supported by the current firmware version.

Start rescue procedure via DHCP/BootP+TFTP
Start rescue procedure from CD / DVD, USB stick or SD Card

“Restart, recovery procedure, and flashing the firmware” on page 247

12.4 Preparing the configuration

12.4.1 Connection requirements

- For the device, the two power supply units must be connected to the power supply source/to the mains. (If only one power supply unit is connected, the device can actually be operated, but it will output an acoustic signal.)
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN port on the device.
- **For remote configuration**: The device must be configured so that remote configuration is permitted.
- The device must be connected, i.e., the required connections must be working.

12.4.2 Local configuration on startup (router mode)

By default upon delivery, following reset to the default settings or after flashing the device, the device can be accessed within the network 192.168.1.0/24 via the LAN interface under IP address 192.168.1.1.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Example

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the “Internet protocol Version 4 (TCP/IPv4)” menu item.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

12.5 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via one of the following addresses:

Table 12-3 Preset addresses

Default setting	Network mode	Management IP #1 (IP address of the internal interface)
FL MGUARD CENTERPORT	Router	https://192.168.1.1/

Proceed as follows:

- Start a HTTP-capable web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 12-3).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 247).

If the administrator web page is not displayed

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

- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.
  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.
  Click on “Properties” under “LAN settings”.
  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.
  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation

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

- Always click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 12-5 Login

- Enter your user name and password which are specified for this access type.

For access type “Administration”, the user name and password are set by default (please note these settings are case-sensitive):

UserName:	admin
Password:	mGuard

The device can then be configured via the web interface.
For additional information, please refer to software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

12.6 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to software reference manual.

12.7 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

12.8 Restart, recovery procedure, and flashing the firmware

The device must be restarted in order to perform a recovery procedure or to flash the firmware.

12.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the ON/OFF button of the device already started for approximately 5 s to switch off the device. (Alternatively, disconnect the power supply and then connect it again.)
- Then press the ON/OFF button again shortly to restart the device.

12.8.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

Use the recovery procedure in case you have forgotten the IP address under which the device can be accessed.

The following network setting is restored:

Table 12-4 Restored network setting

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

The device is reset to router mode with the fixed IP address.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU configuration is activated for the Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

NOTE: After the recovery procedure has been performed successfully, a previously created configuration profile in the device should be loaded and activated again. Then the network settings must be adapted.

Possible reasons for performing the recovery procedure:

– The device is in PPPoE mode.
– The configured IP address of the device differs from the default setting.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. (Application notes are available in the download area at www.innominate.comphoenixcontact.net/products.)

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established

Table 12-5 Restored network setting

Network mode	Management IP #1 (IP address of the internal interface)
Router	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

Requirement: a monitor and a keyboard are connected to the device.

- Press the following keyboard shortcut: <**Alt**>+<**SysRq**>+<**a**>.

(On English keyboards the German <**S-Abf**> corresponds to <**SysRq**>. However, some keyboards do not feature the <**SysRq**> key. In this case, use the <**Print**> key.)

After pressing the keyboard shortcut once, the same shortcut must be pressed again within 30 s in order to start the recovery procedure.

Once the recovery procedure has been performed successfully, a corresponding message appears on the monitor.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

12.8.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

- **All configured settings are deleted.** The device is set to the delivery state.
- In mGuard firmware version 5.0.0 or later, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

There are three options for flashing the firmware:

- Via the network (DHCP and TFTP server)
- Via the USB port (USB Flash drive or USB CD/DVD drive)
- Via the SD memory card

The following requirements apply when loading the firmware from an **SD card**, a **USB Flash drive**:

- 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).
- All necessary firmware files must be located in a common directory on the first partition of the SD card or the USB Flash memory under the following path or in the following folder:
  /Firmware/install.x86_64.p7s
  /Firmware/firmware.img.x86_64.p7s

The following requirements apply when loading the firmware from a **TFTP server**:

- A TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

- The relevant **firmware files** are available for download from the download page of phoenixcontact.net/products.

Preparation

- The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on the installation medium of your choice or on the local installation computer.
- If your current firmware version is newer than the version by default upon delivery, a license must be obtained for using this update. This applies to major release upgrades, e.g., from Version 6.x.y to Version 7.x.y to Version 8.x.y, etc.
- **SD card option**: The SD card has been inserted into the device.
- **USB port option**: A USB Flash drive or a USB CD/DVD driver has been connected to the USB port of the device.
- **Network option**: DHCP and TFTP servers can be accessed under the same IP address.

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: All configured settings are deleted.

The mGuard is set to the delivery state.

In Version 5.0.0 or later of the mGuard, the licenses installed on the mGuard are retained after flashing the firmware. Therefore, they do not have to be installed again.

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

1. Restart/boot the device.
2. As soon as the device boots, press one of the arrow keys on the keyboard several times until the boot process is interrupted: ↑, ↓, ← or →.
3. The boot menu is displayed.

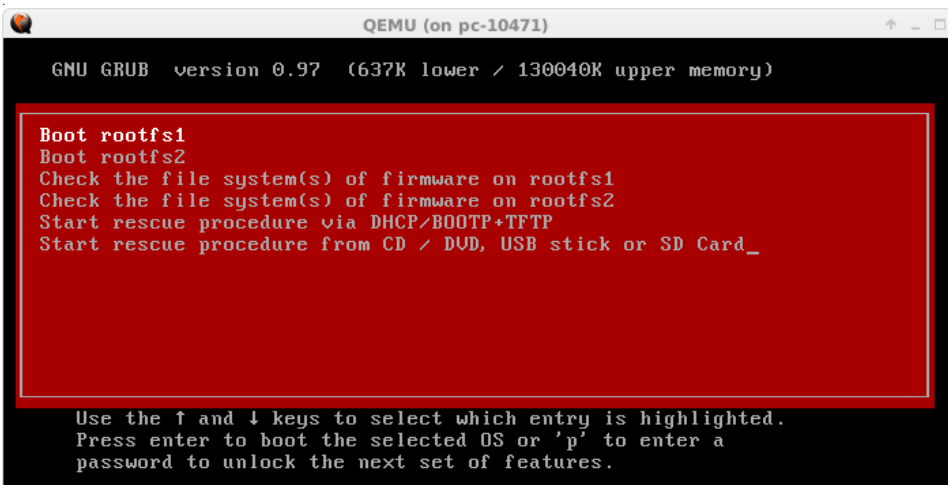


Figure 12-6 FL MGUARD CENTERPORT boot menu

4. Select one of the options to perform the rescue procedure using the arrow keys ↓ or ↑:
   Start rescue procedure via DHCP / BOOTP+TFTP
   OR
   Start rescue procedure from CD / DVD, USB stick or SD Card
   To apply the selection, press the **Enter** key.
   The options include:

Start rescue procedure via DHCP/BootP+TFTP

Effect: The device downloads the necessary files from the TFTP server:
- install.x86_64.p7s
- firmware.img.x86_64.p7s

Start rescue procedure from CD/DVD, USB stick or SD Card

General requirements:

1. A CD/DVD drive connected to the USB port or
2. A USB stick (USB Flash drive) connected to the USB port or
3. An SD memory card inserted into the SD card drive

After the rescue procedure has been started by pressing the Enter key, the required data is downloaded from the medium that was connected/inserted to/into the device.

Start rescue procedure from CD/DVD

Requirement: The firmware of the mGuard has been previously burnt to CD/DVD (see below under “Burning the mGuard firmware to CD/DVD-ROM” on page 252).
Effect: The mGuard device downloads all necessary files from the inserted CD/DVD.
With this in mind, while the boot menu is displayed and before applying this selection, insert the CD/DVD with the mGuard firmware into the CD/DVD drive.
(For security reasons, the FL MGUARD CENTERPORT does not boot from the CD/DVD).

– Once the rescue procedure is complete, a corresponding message appears on the monitor. Follow any further on-screen instructions.

Start rescue procedure from USB stick (USB Flash drive)

Requirement: The firmware of the mGuard has been previously copied to a USB storage medium (USB stick, USB Flash drive).
/Firmware/install.x86_64.p7s
/Firmware/firmware.img.x86_64.p7s
Effect: The mGuard device downloads all necessary files from the connected USB storage medium. (For security reasons, the FL MGUARD CENTERPORT does not boot from the USB storage medium).

– Once the rescue procedure is complete, a corresponding message appears on the monitor. Follow any further on-screen instructions.

Start rescue procedure from SD Card

Requirement: The firmware of the mGuard has been previously copied to the SD card:
/Firmware/install.x86_64.p7s
/Firmware/firmware.img.x86_64.p7s
Effect: The mGuard device downloads all necessary files from the inserted SD card. With this in mind, while the boot menu is displayed at the latest and before applying this selection, insert the SD card with the stored firmware into the device. (For security reasons, the FL MGUARD CENTERPORT does not boot from an SD card).

– Once the rescue procedure is complete, a corresponding message appears on the monitor. Follow any further on-screen instructions.

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 244):

Burning the mGuard firmware to CD/DVD-ROM

The firmware for the mGuard can be burnt to CD/DVD. A zip file is available for download from the download page of phoenixcontact.net/products.

Burn the content of this zip archive as a data CD/DVD. The following files must be located in the following folders/under the following path names on the CD/DVD:

– /Firmware/install.x86_64.p7s
– /Firmware/firmware.img.x86_64.p7s

12.9 Technical data

Hardware properties	FL MGUARD CENTERPORT
Platform	Multi-core x86 processor architecture
Network interfaces	1 LAN port I 1 WAN port I 1 SYNC port I 1 DMZ port Ethernet IEEE 802.3 10/100/1000 Base TX I RJ45 I full/half duplex I auto MDIX
Other interfaces	VGA console I serial RS-232, D-SUB 9 connector I 6 x USB
Drives	1 HDD I 1 SD card
Redundancy options	Optional VPN license I router and firewall
Power supply	2 x 100 V AC ... 240 V AC, 300 W at 50/60 Hz, redundant
Power consumption	Dependent on the expansion stage
Humidity range	20% ... 90% during operation, non-condensing 10% ... 90% out of service
Degree of protection	Front IP20
Temperature range	0°C ... +45°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	44 mm x 447 mm x 458 mm (1 HU x 19" x 18.5")
Weight	17 kg

Firmware and power values	FL MGUARD CENTERPORT
Firmware compatibility	mGuard v8.1.2 or later; Phoenix Contact recommends using the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet or the corresponding release notes.
Data throughput (router I firewall)	2,000 Mbps bidirectional I 2,000 Mbps bidirectional When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.
Hardware-based encryption	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	600 Mbps bidirectional (router mode) When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	Dot matrix display I LEDs I boot menu I log file I remote Syslog

Other	FL MGUARD CENTERPORT
Conformance	FCC, CE, developed according to UL requirements

13 FL MGUARD DELTA TX/TX

Table 13-1 Currently available products

Product designation	Phoenix Contact order number
FL MGUARD DELTA TX/TX	2700967
FL MGUARD DELTA TX/TX VPN	2700968

Product description

The **FL MGUARD DELTA TX/TX** is ideal for use in desktop applications, in distribution compartments, and other environments close to production processes with low requirements for industrial hardening.

Individual devices or network segments can be safely networked and comprehensively protected. The FL MGUARD DELTA TX/TX can be used as a firewall between office and production networks as well as a security router for small and medium-sized workgroups.

Figure 13-1 FL MGUARD DELTA TX/TX

13.1 Operating elements and LEDs

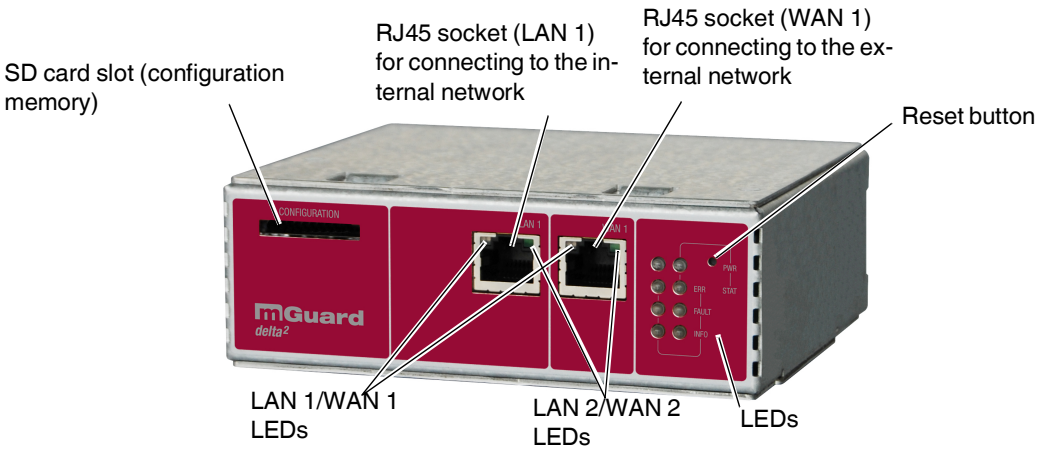


Figure 13-2 Operating elements and LEDs on the

Table 13-2 LEDs on the FL MGUARD DELTA TX/TX

LEDs	State		Meaning
WAN 1	Green	On	Full duplex
LAN 1		Off	Half duplex
WAN 2	Yellow	On	10 Mbps
LAN 2		Flashing	10 Mbps, data transmission active
	Green	On	100 Mbps
		Flashing	100 Mbps, data transmission active
PWR	Green	On	Supply voltage OK
STAT	Green	Flashing	The mGuard is ready to operate.
ERR	Red	On	System error
FAULT	Red	On	mGuard in the booting or flashing state
INFO			Not used

13.2 Startup

13.2.1 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: Risk of material damage due to incorrect wiring

Only connect the device network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the device.

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  0°C ... +40°C
– Maximum humidity, non-condensing:
  5% ... 95%
  To avoid overheating, do not expose the device to direct sunlight or other heat sources.

NOTE: Cleaning

Clean the device housing with a soft cloth. Do not use aggressive solvents.

13.2.2 Checking the scope of supply

Before startup, check the scope of supply to ensure nothing is missing.

The scope of supply includes:

– FL MGUARD DELTA TX/TX
– Package slip
– 12 V DC power supply including different country adapters

13.3 Connecting the FL MGUARD DELTA TX/TX

NOTE: Notes on mounting and installation

Only connect the RJ45 Ethernet ports of the device to matching network installations. Some telecommunications connections also use RJ45 sockets. You may not connect these to the RJ45 ports of the device.

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.

13.3.1 Connecting to the network

- Connect the device to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply.
- Connect the internal network interface LAN 1 of the device to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

13.3.2 Connecting the supply voltage

- Connect the wide-range power supply unit of the device to a suitable power supply. Connect the low-voltage plug of the power supply unit on the back of the device.

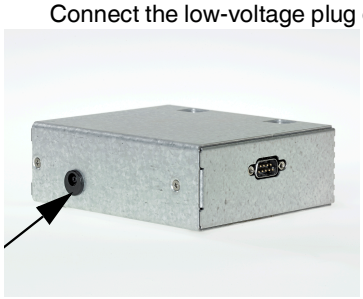


Figure 13-3 Low-voltage plug of the power supply unit

The status LED PWR lights up green when the supply voltage has been connected properly.

The device boots the firmware. Status LED STAT flashes green.

The device is ready for operation as soon as the LAN/WAN LEDs of the Ethernet socket light up.

Additionally, the status LED PWR lights up green and the status LED STAT flashes green at heartbeat.

13.4 Preparing the configuration

13.4.1 Connection requirements

FL MGUARD DELTA TX/TX

- The FL MGUARD DELTA TX/TX must be connected to its power supply.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
- **For remote configuration**: The device must be configured so that remote configuration is permitted.
- The device must be connected, i.e., the required connections must be working.

13.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The device is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the device can be accessed via the following addresses:

Table 13-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (in the web interface under “Network >> Interfaces >> General”). Alternatively, you can select a different stealth configuration or use another network mode.

13.5 Configuration in Stealth mode

On initial startup, the device can be accessed via two addresses:

– https://192.168.1.1/ (see Page 261)
– https://1.1.1.1/ (see Page 261)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 262).

The device can be accessed via https://192.168.1.1/ if the external network interface is not connected on startup.

Computers can access the device via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the device. For this purpose, the device with LAN port and WAN port must be integrated in an operational network in which the default gateway can be accessed via the WAN port.

– After access via IP address 192.168.1.1 and successful login, IP address 192.168.1.1 is set as a fixed management IP address.
– After access via IP address 1.1.1.1 or after IP address assignment via BootP, the FL MGUARD can no longer be accessed via IP address 192.168.1.1.

13.5.1 IP address 192.168.1.1

In Stealth mode, the device can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.

– The device is in the delivery state.
– The device was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the device) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard device in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the device, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

13.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the device to be addressed via address **https://1.1.1.1/**, it must be connected to a configured network interface. This is the case if it is connected in an existing network connection and if the default gateway can be accessed via the WAN port of the device at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 263). Continue from this point.

After access via IP address 1.1.1.1, the FL MGUARD can no longer be accessed via IP address 192.168.1.1

13.5.3 Assigning the IP address via BootP

After assigning an IP address via BootP, the FL MGUARD can no longer be accessed via IP address 192.168.1.1

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

Section 14.1 explains IP address assignment using the free Windows software "IP Assignment Tool" (IPAssign.exe).

Notes for BootP

During initial startup, the device transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the device no longer sends BootP requests. The FL MGUARD 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) must be performed.

13.6 Establishing a local configuration connection

Web-based administrator interface

The device is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The device can be accessed via one of the following addresses:

Table 13-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the device may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 13-4).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 267).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 259).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.
  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.
  Click on “Properties” under “LAN settings”.
  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.
  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

Figure 13-4 Login

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

User Name:	admin
Password:	mGuard

The device can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

13.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

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, 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. For additional information, please refer to the software reference manual.

13.8 Serial interface

Via the serial interface (RS232), a user can access the command line of the device. The following parameters must be configured device-specific:

– Baud rate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware handshake RTS/CTS: Off (default)

13.9 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure

Figure 13-5 Reset button

13.9.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the ERR LED lights up. (Alternatively, disconnect the power supply and then connect it again.)

13.9.2 Performing a recovery procedure

Objective (up to 8.3.x)

Up to mGuard firmware version 8.3.x

The network configuration (but not the rest of the configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

When performing the recovery procedure, the default network settings are established:

Table 13-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

The device is reset to Stealth mode with the default setting “multiple Clients”.

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
– In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The device is in Router or PPPoE mode.
– The configured IP address of the device differs from the default setting.
– The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version. You can find application notes under the following Internet address: phoenixcontact.net/products.

Objective (8.4.0 or later)

mGuard firmware version 8.4.0 or later

The complete configuration (and not only the network configuration) is to be reset to the delivery state, as it is no longer possible to access the device.

The current configuration will be automatically be saved on the device and can be restored after the recovery procedure is finished.

When performing the recovery procedure, the default network settings are established:

Table 13-6 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

Activity during the recovery procedure (mGuard firmware version 8.4.0 or later)

Before performing the recovery procedure, the current configuration of the device is stored in a newly generated configuration profile ("Recovery-DATE"). After the recovery procedure has finished, the device starts with the Factory Default settings.

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

Action

- Slowly press the Reset button six times.
  After approximately 2 seconds, the STAT LED lights up green.
- Slowly press the Reset button again six times.
  If successful, the STAT LED lights up green.
  If unsuccessful, the ERR LED lights up red.

If successful, the device restarts after two seconds and switches to Stealth mode. The device can then be reached again under the corresponding addresses.

mGuard firmware version 8.4.0 or later

- After the recovery procedure has finished, log in to the web interface of the device.
- Open the menu **Management >> Configuration Profiles**.
- Choose the configuration profile, generated during the recovery procedure: „Recovery-DATE“ (e.g. “Recovery-2016.12.01-18:02:50).
- Click on the Icon „Edit profile“ to analyze the configuration profile and to restore it with or without changes.
- Click on the Icon „Save“ to apply the changes.

13.9.3 Flashing the firmware/rescue procedure

For further information, see also the Application Note Update and Flash FL/TC MGUARD Devices, available at phoenixcontact.net/products.

Objective

The entire mGuard firmware should be reloaded on the device.

- **All configured settings are deleted.** The device is set to the delivery state.
- In mGuard firmware version 5.0.0 or later, the licenses installed on the device are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

The following requirements apply when loading the firmware from an SD card:

- All necessary firmware files must be located in a common directory on the first partition of the SD card.
- This partition must use a VFAT file system (standard type for SD cards).

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 276).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

- The mGuard firmware has been obtained from your dealer's support team or the phoenixcontact.net/products website and has been saved on a compatible SD card.
- This SD card has been inserted into the device.
- The relevant firmware files are available for download from the download page of phoenixcontact.net/products. The files must be located under the following path names or in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s

  Firmware/ubifs.img.mpc83xx.p7s

Action

To flash the firmware or to perform the rescue procedure, proceed as follows:

NOTE: Do not interrupt the power supply to the device during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the STAT, MOD, and SIG LEDs light up green. Then, the device is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the device is restarted.

  The device now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The STAT LED flashes.

  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.

  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.

  The STAT, MOD, and SIG LEDs form a running light.

  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Phoenix Contact are accepted.

  This process takes around 3 to 5 minutes. The STAT LED is lit continuously.

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.

As soon as the procedure is complete, the STAT, MOD, and SIG LEDs flash green simultaneously.

- Restart the device. To do this, briefly press the Reset button.

  (Alternatively, disconnect the power supply and then connect it again.)

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 263):

13.10 Technical data

Hardware properties	FL MGUARD DELTA TX/TX
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232, D-SUB 9 connector
Memory	128 MB RAM I 128 MB Flash SD card, replaceable configuration memory
Redundancy options	Optional: VPN I router
Power supply	External power supply unit 12 V/0.85 A DC I 100 – 240 V/0.4 A AC
Power consumption	2.13 W, typical
Humidity range	5% ... 95% during operation, non-condensing
Degree of protection	IP20
Temperature range	0°C ... +40°C (operation) 0°C ... +60°C (storage)
Dimensions (H x W x D)	45 x 130 x 114 mm
Weight	725 g
Weight (incl. packaging)	1025 g

Firmware and power values	FL MGUARD DELTA TX/TX
Firmware compatibility	For mGuard v7.4.0 or later: Phoenix Contact recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (Firewall)	Router mode, default firewall rules, bidirectional throughput: max. 120 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 50 Mbps
Virtual Private Network (VPN)	IPsec (IETF standard), VPN models up to 10 tunnels, Optionally up to 250 VPN tunnels
Hardware-based encryption	DES I 3DES I AES-128/192/256
Data throughput encrypted (IPsec VPN)	Router mode, default firewall rules, bidirectional throughput: max. 30 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 20 Mbps
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (Power, State, Error, Signal, Fault, Info) I log file I remote syslog

Other	FL MGUARD DELTA TX/TX
Conformance	CE I FCC
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Remote Services Portal ready

14 Assigning IP addresses and setting up DHCP/TFTP servers

14.1 Assigning the IP address using IPAssign.exe

Step 1: Downloading and executing the program

- On the Internet, select the link phoenixcontact.net/products.
- Enter the keyword „ipassign“ in the search field.
- Chose the desired or any other product.

The desired program can be found under “Download” and “Software”.

- Double-click on the “IPAssign.exe” file.
- In the window that opens, click on “Run”.

Step 2: “IP Assignment Tool”

The program opens and the start screen of the addressing tool appears.

The program is mainly in English. However, the program buttons change according to the country-specific settings.

The start screen displays the IP address of the PC. This helps when addressing the mGuard in the subsequent steps.

- Click on “Next”.

Step 3: “IP Address Request Listener”

All devices sending a BootP request are listed in the window which opens. These devices are waiting for a new IP address.

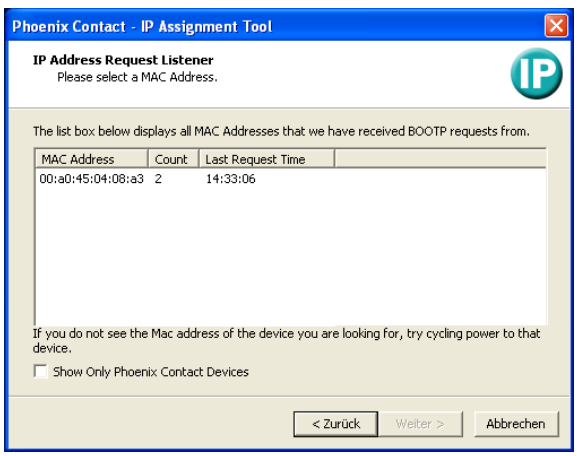


Figure 14-1 “IP Address Request Listener” window

In this example, the mGuard has MAC ID 00.A0.45.04.08.A3.

- Select the device to which you would like to assign an IP address.
- Click on “Next”.

Step 4: “Set IP address”

The following information is displayed in the window which opens:

– IP address of the PC
– MAC address of the selected device
– IP parameters of the selected device
(IP address, subnet mask, and gateway address)
– Any incorrect settings

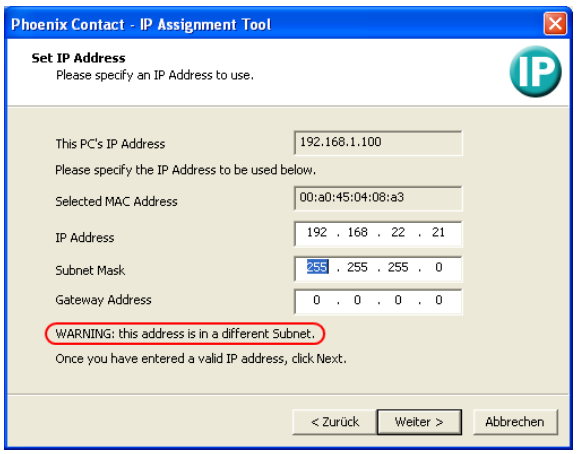


Figure 14-2 “Set IP Address” window with incorrect settings

- Adjust the IP parameters according to your requirements.

If inconsistencies are no longer detected, a message appears indicating that a valid IP address has been set.

- Click on “Next”.

Step 5: “Assign IP address”

The program attempts to transmit the IP parameters set to the mGuard.

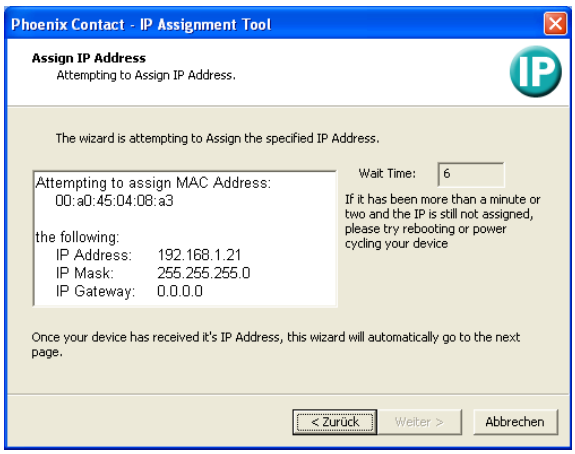


Figure 14-3 “Assign IP address” window

Following successful transmission, the next window opens.

Step 6: Finishing IP address assignment

The window that opens informs you that address assignment has been successfully completed. It gives an overview of the IP parameters that have been transmitted to the device with the MAC address shown.

To assign IP parameters for additional devices:

- Click on “Back”.

To exit IP address assignment:

- Click on “Finish”.

If required, the IP parameters set here can be changed on the mGuard web interface under “Network >> Interfaces”.

14.2 Installing the DHCP and TFTP server

Installing a second DHCP server in a network could affect the configuration of the entire network.

Third-party software

Phoenix Contact assumes no guarantee or liability for the use of third-party products. References to third-party software are not a recommendation. They represent examples of generally usable programs.

Under Windows

If you want to use the third-party program „TFTPD32.exe“, obtain the program from a trusted source and proceed as follows:

- If the Windows computer is connected to a network, disconnect it from the network.
- Copy the firmware to an empty folder on the Windows computer.
- Start the „TFTPD32.exe“ programm.

The host IP to be specified is: **192.168.10.1.** It must also be used as the address for the network card.

- Click on **Browse** to switch to the folder where the mGuard image files are saved: **install.p7s, jffs2.img.p7s**
- If a major release upgrade of the firmware is carried out by flashing, the license file purchased for the upgrade must also be stored here under the name **licence.lic** or the serial number of the corresponding device **<serialnumber>.lic** (e.g. 2138413892.lic)

  Make sure that this is the correct license file for the device (under “Management >> Update” on the web interface).

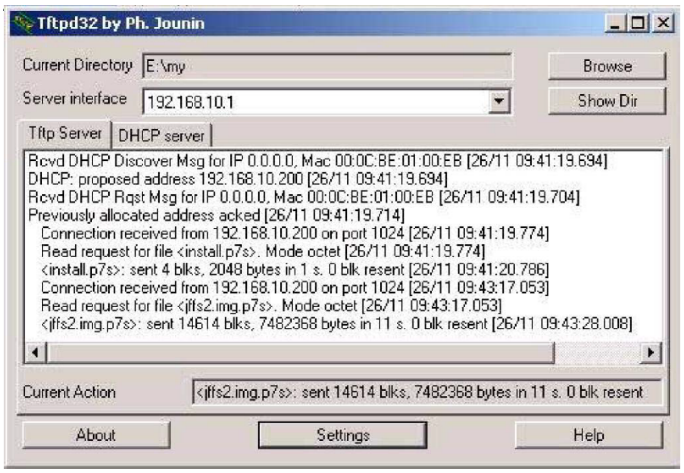
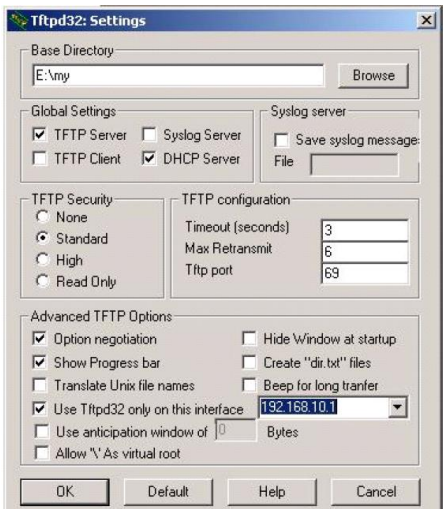


Figure 14-4 Entering the host IP

- Switch to the “TFTP Server” or “DHCP Server” tab page and click on “Settings” to set the parameters as follows:



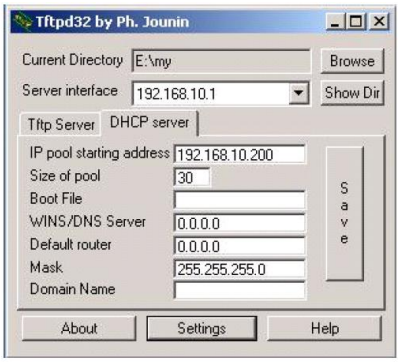


Figure 14-5 Settings

Under Linux

All current Linux distributions include DHCP and TFTP servers.

- Install the corresponding packages according to the instructions provided for the relevant distribution.
- 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**

- 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:
install.p7s, jffs2.img.p7s

- If a major release upgrade of the firmware is carried out by flashing, the license file purchased for the upgrade must also be stored here under the name **licence.lic** or the serial number of the corresponding device **<serialnumber>.lic** (e.g. 2138413892.lic).

  Make sure that this is the correct license file for the device (under “Management >> Update” on the web interface).
- Then restart the inetd process to apply the configuration changes.
- When using a different mechanism, e.g., xinetd, please consult the relevant documentation.