Chipsmall
深圳市津利帝科技有限公司
Geelead Technology Limited
Chipsmall
采购部

AUTOMATION

User manual

UM EN FL MGUARD2

Order No.: —

User manual for the hardware and software of FL MGUARD security appliances

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATION

User manual

User manual for the hardware and software of FL MGUARD security appliances

2012-06-27

Designation:	UM EN FL MGUARD2
Revision:	01
Order No.:	—

This user manual is valid for:

Designation	Revision	Order No.
FL MGUARD RS2000 TX/TX VPN		2700642
FL MGUARD RS4000 TX/TX		2700634
FL MGUARD RS4000 TX/TX VPN		2200515
FL MGUARD SMART2		2700640
FL MGUARD SMART2 VPN		2700639
FL MGUARD DELTA TX/TX		2700967

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.
- Qualified application programmers and software engineers, who are familiar with the safety concepts of automation technology and applicable standards.

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.

ℹ 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 Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
www.phoenixcontact.com

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

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 www.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

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

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

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

This manual, including all illustrations contained herein, is copyright protected. Any changes to the contents or the publication of extracts of this document is prohibited.

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

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

Table of contents

1 Introduction

The FL MGUARD protects IP data links by combining the following functions:

- VPN router (VPN - **V**irtual **P**rivate **N**etwork) for secure data transmission via public networks (hardware-based DES, 3DES, and AES encryption, IPsec protocol).
- Configurable firewall for protection against unauthorized access. The dynamic packet filter inspects data packets using the source and destination address and blocks undesired data traffic.

The device can be configured easily using a web browser.

Further information can be found on our website at www.phoenixcontact.com.

Network features

- Stealth (auto, static, multi), router (static, DHCP client), PPPoE (for DSL), PPTP (for DSL), and modem mode
- VLAN
- DHCP server/relay on internal and external network interfaces
- DNS cache on the internal network interface
- Administration via HTTPS and SSH
- Optional conversion of DSCP/TOS values (Quality of Service)
- Quality of Service (QoS)
- LLDP
- MAU management
- SNMP

Firewall features

- Stateful packet inspection
- Anti-spoofing
- IP filter
- L2 filter (only in stealth mode)
- NAT with FTP, IRC, and PPTP support (only in router modes)
- 1:1 NAT (only in *router* network mode)
- Port forwarding (not in *stealth* network mode)
- Individual firewall rules for different users (user firewall)
- Individual rule sets as action (target) of firewall rules (apart from user firewall or VPN firewall)

Anti-virus features (optional)

- CIFS integrity check of network drives for changes to specific file types (e.g., executable files)
- Anti-virus scan connector which supports central monitoring of network drives with virus scanners

VPN features

- Protocol: IPsec (tunnel and transport mode)
- IPsec encryption in hardware with DES (56 bits), 3DES (168 bits), and AES (128, 192, 256 bits)
- Packet authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with main and quick mode
- Authentication via:
  - Pre-shared key (PSK)
  - X.509v3 certificates with public key infrastructure (PKI) with certification authority (CA), optional certificate revocation list (CRL), and the option of filtering by subject

  or
  - Partner certificate, e.g., self-signed certificates
- Detection of changing partner IP addresses via DynDNS
- NAT traversal (NAT-T)
- Dead Peer Detection (DPD): detection of IPsec connection aborts
- IPsec/L2TP server: connection of IPsec/L2TP clients
- IPsec firewall and 1:1 NAT
- Default route over VPN
- Data forwarding between VPNs (hub and spoke)
- Dependent on the license: Up to 250 VPN channels, hardware acceleration for encryption in VPN additional features
- Remote logging
- Router/firewall redundancy (optional)
- Administration using SNMP v1-v3 and device manager software (FL MGUARD DM...)
- PKI support for HTTPS/SSH remote access
- Can act as an NTP and DNS server via the LAN interface

Support

In the event of problems with your FL MGUARD, please contact your dealer.

Additional information on the device as well as on release notes and software updates can be found on the Internet at www.phoenixcontact.com.

1.1 Device versions

The **FL MGUARD** is available in the following device versions, which largely have identical functions. All devices can be used regardless of the processor technology and operating system used by the connected computers.

FL MGUARD SMART2

The **FL MGUARD SMART2** is the smallest device version. For example, it can be easily inserted between the computer or local network (at the LAN port of the FL MGUARD) and an available router (at the WAN port of the FL MGUARD), 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.

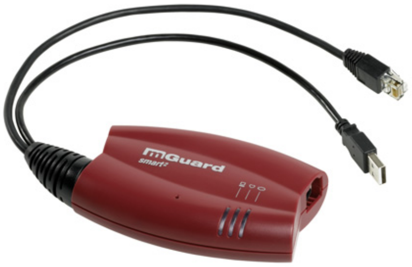


Figure 1-1 FL MGUARD SMART2

FL MGUARD RS4000/ FL MGUARD RS2000

The FL MGUARD RS4000 is a security appliance with intelligent firewall and optional IPsec VPN (10 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 security router 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 have a replaceable configuration memory (SD card). 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		

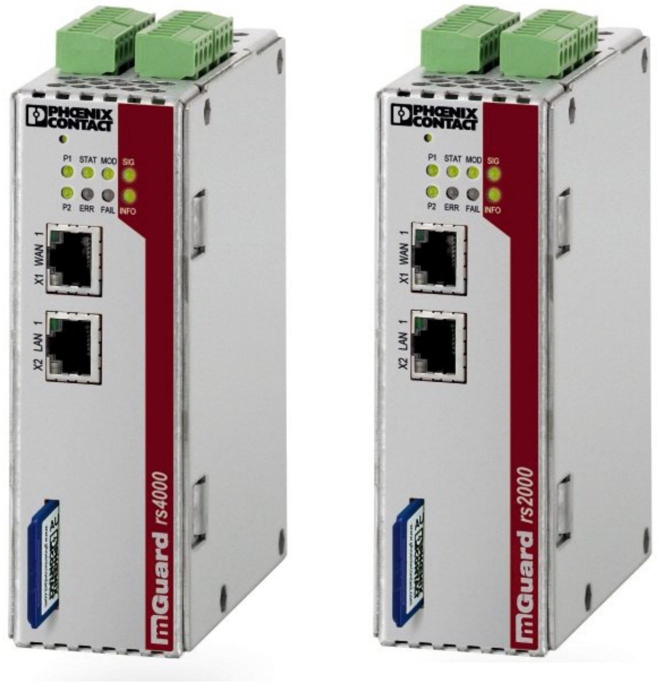


Figure 1-2 FL MGUARD RS4000/FL MGUARD RS2000

2 Preliminary user manualTypical application scenarios

This section describes various application scenarios for the FL MGUARD.

- Stealth mode
- Network router
- DMZ
- VPN gateway
- WLAN via VPN
- Resolving network conflicts

2.1 Stealth mode

In **stealth mode**, the FL MGUARD can be positioned between an individual computer and the rest of the network.

The settings (e.g., for firewall and VPN) can be made using a web browser under the URL https://1.1.1.1/.

No configuration modifications are required on the computer itself.

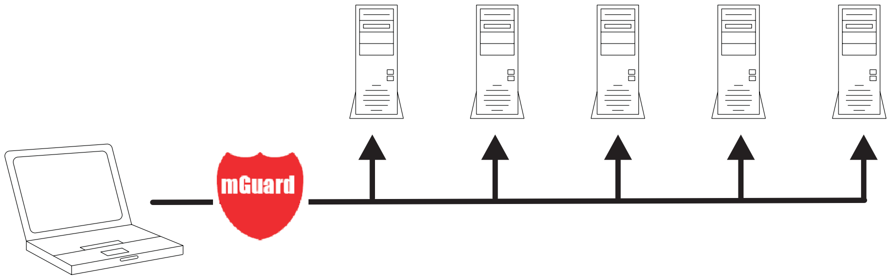


Figure 2-1 Stealth mode

2.2 Network router

When used as a **network router**, the FL MGUARD can provide the Internet link for several computers and protect the company network with its firewall.

One of the following network modes can be used on the FL MGUARD:

- *Router*, if the Internet connection is, for example, via a DSL router or a permanent line.
- *PPPoE*, if the Internet connection is, for example, via a DSL modem and the PPPoE protocol is used (e.g., in Germany).
- *PPTP*, if the Internet connection is, for example, via a DSL modem and the PPTP protocol is used (e.g., in Austria).
- *Modem*, if the Internet connection is via a serial connected modem (compatible with Hayes or AT command set).

For computers in the Intranet, the FL MGUARD must be specified as the default gateway.

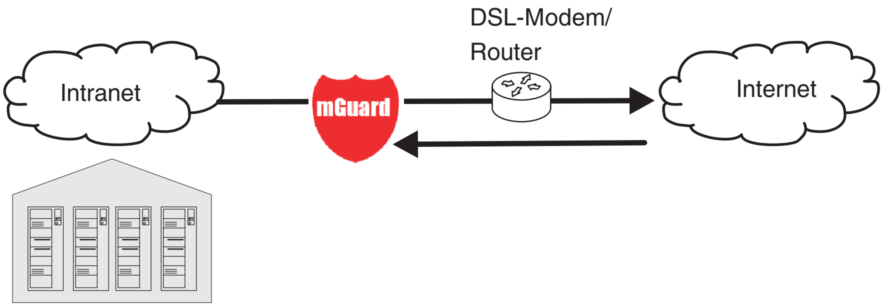


Figure 2-2 Network router

2.3 DMZ

A **DMZ** (demilitarized zone) is a protected network that is located between two other networks. For example, a company's website may be in the DMZ so that new pages can only be copied to the server from the Intranet using FTP. However, the pages can be read from the Internet via HTTP.

IP addresses within the DMZ can be public or private, and the FL MGUARD, which is connected to the Internet, forwards the connections to private addresses within the DMZ by means of port forwarding.

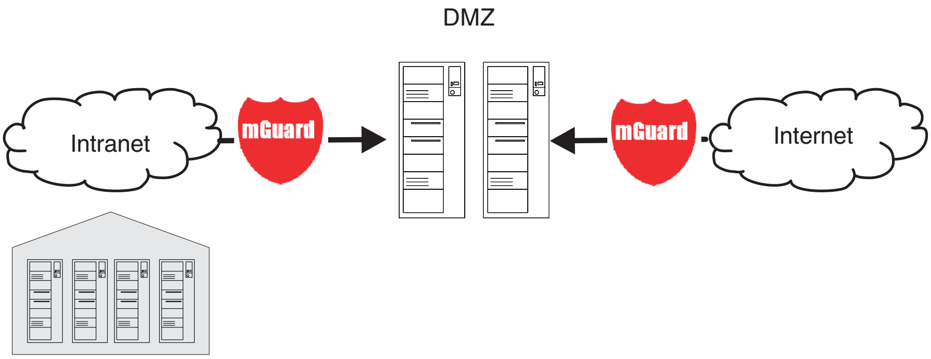


Figure 2-3 DMZ

2.4 VPN gateway

The **VPN gateway** provides company employees with encrypted access to the company network from home or when traveling. The FL MGUARD performs the role of the VPN gateway.

IPsec-capable VPN client software must be installed on the external computers and the operating system must support this functionality. For example, Windows 2000/XP can be used or the computer can be equipped with an FL MGUARD.

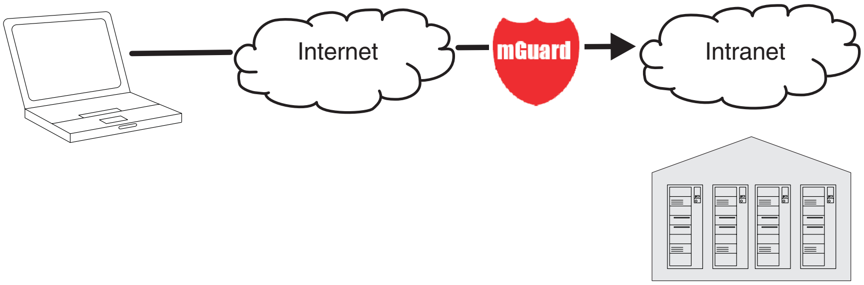


Figure 2-4 VPN gateway

2.5 WLAN via VPN

WLAN via VPN is used to connect two company buildings via a WLAN path protected using IPsec. The annex should also be able to use the Internet connection of the main building.

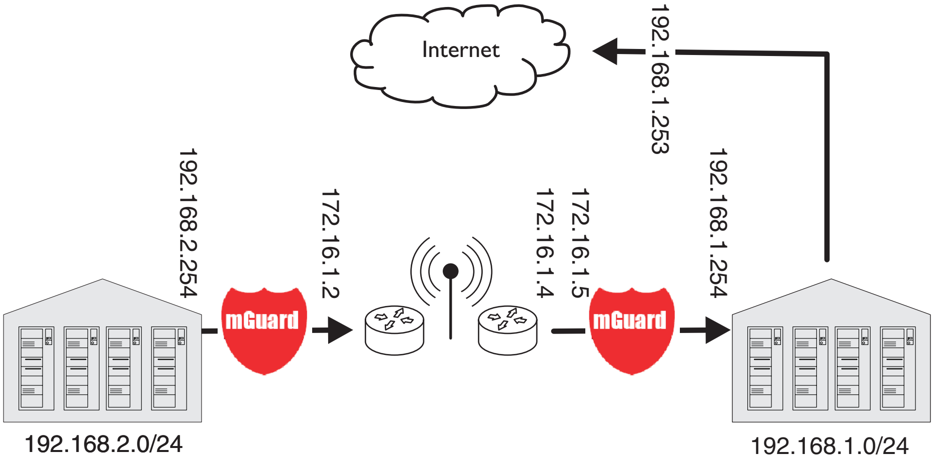


Figure 2-5 WLAN via VPN

In this example, the FL MGUARD devices were set to *router* mode and a separate network with 172.16.1.x addresses was set up for the WLAN.

To provide the annex with an Internet connection via the VPN, a default route is set up via the VPN:

Tunnel configuration in the annex

Connection type	Tunnel (network <-> network)
Address of the local network	192.168.2.0/24
Address of the remote network	0.0.0.0/0

In the main building, the corresponding counterpart is configured:

Tunnel configuration in the main building

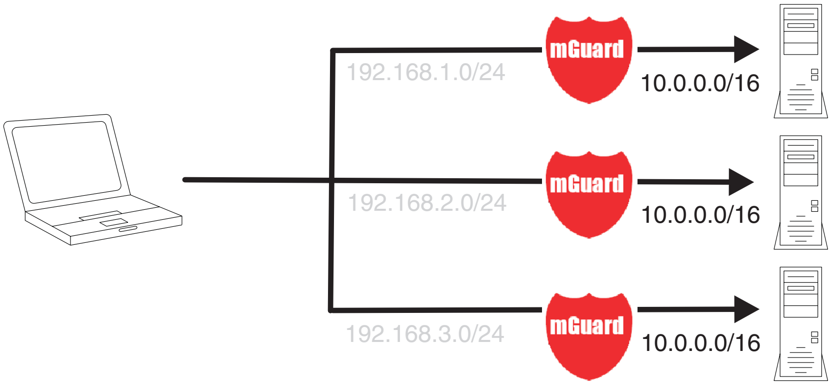
Connection type	Tunnel (network <-> network)
Local network	0.0.0.0
Address of the remote network	192.168.2.0/24

The default route of an FL MGUARD usually uses the WAN port. However, in this case the Internet can be accessed via the LAN port:

Default gateway in the main building

IP address of the default gateway	192.168.1.253

2.6 Resolving network conflicts



Resolving network conflicts

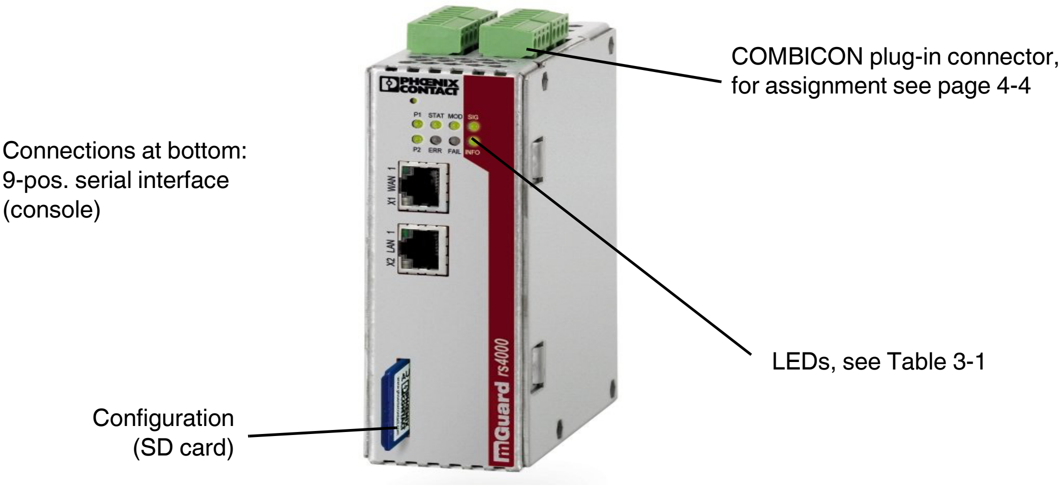
In the example, the networks on the right-hand side should be accessible to the network or computer on the left-hand side. However, for historical or technical reasons the networks on the right-hand side overlap.

The 1:1 NAT feature of the FL MGUARD can be used to translate these networks to other networks, thus resolving the conflict.

(1:1 NAT can be used in normal routing and in IPsec tunnels.)

3 Operating elements and LEDs

3.1 FL MGUARD RS4000/RS2000



COMBICON plug-in connector,
for assignment see page 4-4

Connections at bottom:
9-pos. serial interface
(console)

LEDs, see Table 3-1

Configuration
(SD card)

Figure 3-1 Operating elements and LEDs on the FL MGUARD RS4000

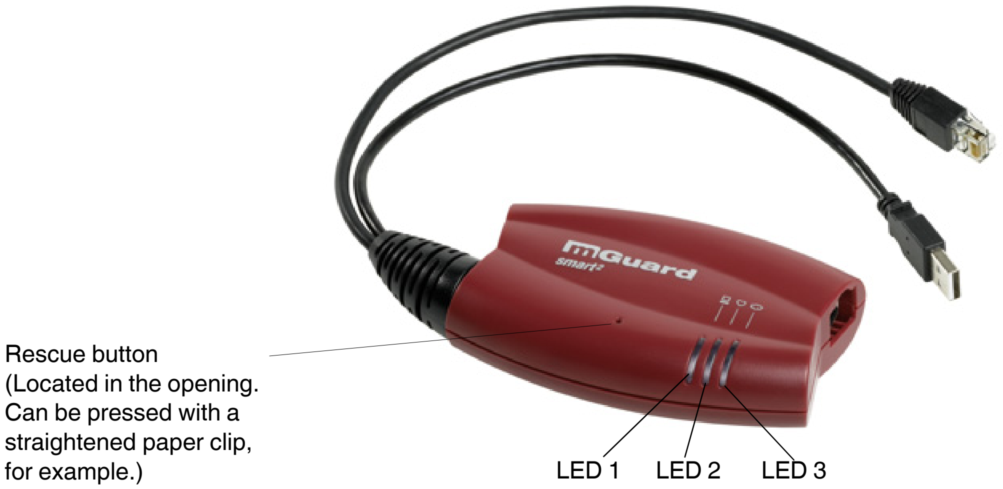
Table 3-1 LEDs on the FL MGUARD RS4000 and RS2000

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	Flashing green	**Heartbeat**. The device is connected correctly and is operating.
ERR	Flashing red	**System error**. Restart the device. – Press the Rescue 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 8-2) or contact the Support team.
SIG	–	(Not used)
FAULT	Red ON	The alarm output is open due to an error (see “Installing the FL MGUARD RS4000/RS2000” on page 4-3). (The alarm output is interrupted during a restart.)
MOD	Green ON	Connection via modem established
INFO	–	(Not used)

Table 3-1 LEDs on the FL MGUARD RS4000 and RS2000 [...]

LED	State	Meaning
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.
LAN	Green ON	The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED) **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.
WAN	Green ON	

3.2 FL MGUARD SMART2



Rescue button (Located in the opening. Can be pressed with a straightened paper clip, for example.)

Figure 3-2 Operating elements and LEDs on the FL MGUARD SMART2

Table 3-2 LEDs on the FL MGUARD SMART2

LEDs	Color	State	Meaning
2	Red/green	Flashing red/green	**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
	Green	Flashing	**Heartbeat**. The device is connected correctly and is operating.
	Red	Flashing	**System error**. Restart the device. • Press the Rescue 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 8-2) or contact the Support team.
1 and 3	Green	ON or flashing	**Ethernet status**. LED 1 indicates the status of the LAN port, LED 3 the status of the WAN port. As soon as the device is connected to the network, a continuous light indicates that there is a connection to the network partner. When data packets are transmitted, the LED goes out briefly.
1, 2, 3	Various LED light codes		**Recovery mode**. After pressing the **Rescue** button. See “Restart, recovery procedure, and flashing the firmware” on page 8-1.

4 Startup

4.1 Safety notes

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

WARNING: Intended use

Only use the FL MGUARD in an appropriate way and for its intended purpose.

WARNING: Only connect LAN installations to RJ45 female connectors

Only connect the FL MGUARD network ports to LAN installations. Some telecommunications connections also use RJ45 female connectors; these must not be connected to the RJ45 female connectors of the FL MGUARD.

Please also note the additional safety notes for the device in the following sections.

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C to +40°C (FL MGUARD SMART2),
  -20°C to +60°C (FL MGUARD RS4000/FL MGUARD RS2000),
  0°C to +40°C (FL MGUARD DELTA TX/TX),
- Maximum humidity 90%, non-condensing
  (FL MGUARD SMART2)
  Maximum humidity 95%, non-condensing
  (FL MGUARD RS4000/FL MGUARD RS2000/FL MGUARD DELTA TX/TX)

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

NOTE: Cleaning

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

Steps for startup

To start up the device, carry out the following steps in the specified order:

Table 4-1 Steps for startup

Step	Aim	Page
1	Check the scope of supply Read the release notes	“Checking the scope of supply” on page 4-2
2	Connect the device	“Connecting the FL MGUARD SMART2” on page 4-7 “Installing the FL MGUARD RS4000/RS2000” on page 4-3
3	Configure the device, if required. Work through the individual menu options offered by the FL MGUARD configuration interface. Read the explanations in this user manual in order to determine which settings are necessary or desirable for your operating environment.	“Local configuration on startup (EIS)” on page 5-2

4.2 Checking the scope of supply

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

The scope of supply includes:

- The FL MGUARD SMART2, FL MGUARD RS4000 or FL MGUARD RS2000 device
- Package slip

The FL MGUARD RS4000 and FL MGUARD RS2000 also include:

- COMBICON plug-in connector for the power supply connection and inputs/outputs (inserted)

4.3 Installing the FL MGUARD RS4000/RS2000

4.3.1 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.

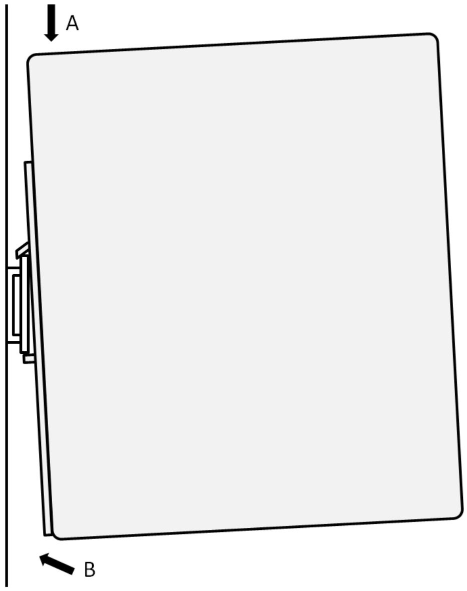


Figure 4-1 Mounting the FL MGUARD RS4000/RS2000 on a DIN rail

- 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 pull up the FL MGUARD RS4000/RS2000.

4.3.2 Connecting to the network

WARNING:

Only connect the FL MGUARD network ports to LAN installations.

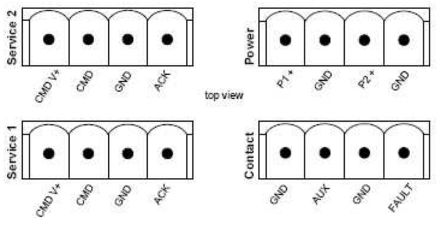
Some telecommunications connections also use RJ45 female connectors; these must not be connected to the RJ45 female connectors of the FL MGUARD.

- Connect the FL MGUARD 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 FL MGUARD to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network (LAN).

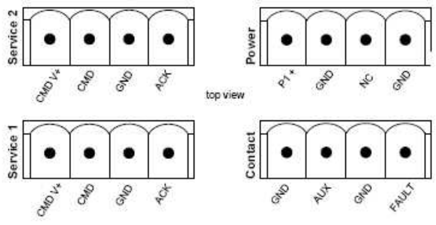
4.3.3 Service contacts

WARNING: The service contacts (GND, CMD, CMD V+, ACK) must not be connected to an external voltage source; they should always be connected as described here.

Please note that only the "Service 1" contacts are used with firmware version 7.4. The "Service 2" contacts shall be made available with a later firmware version.



FL MGUARD RS4000



FL MGUARD RS2000

Table 4-2 **Service 1** plug pin assignment

Designation	Function	Use
CMD V+	Switch contact pin 1	VPN enable switch
CMD	Switch contact pin 2	VPN enable switch
GND	Signal contact -	VPN status light
ACK	Signal contact + (9 to 36 V)	VPN status light

Table 4-3 **Service 2** plug pin assignment

Designation	Function	Use
CMD V+	Not used	None, at present
CMD	Not used	None, at present
GND	Not used	None, at present
ACK	Not used	None, at present

Table 4-4 **Contact** plug pin assignment

Designation	Function	Use
GND	Not used	None, at present
OFF	Not used	None, at present
GND	Alarm contact -	E.g., as error light
FAULT	Alarm contact + (9 to 36 V) Voltage present when operating correctly; disconnected in the event of a fault	E.g., as error light

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

A standard lamp (24 V) can be connected between **contacts ACK (+) and GND (-)**. The contact is short-circuit-proof and supplies a maximum of 250 mA.

The **button** or **on/off switch** is used to establish and release a predefined VPN connection. The output indicates the status of the VPN connection (see "IPsec VPN >> Global" on page 6-163 under "Options").

Operating a connected button

- To establish the VPN connection, hold down the button for a few seconds until the signal output flashes. Then release the button.
  Flashing indicates that the FL MGUARD has received the command to establish the VPN connection and is establishing the VPN connection. As soon as the VPN connection is established, the signal output remains lit continuously.
- To release the VPN connection, hold down the button for a few seconds until the signal output flashes or goes out. Then release the button.
  As soon as the signal output 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 signal output is OFF, 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 ON, the VPN connection is present.

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

4.3.4 Connecting the supply voltage

⚠

WARNING:

The FL MGUARD RS4000/RS2000 is designed for operation with a DC voltage of 9 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 alarm contact.