



Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!



Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832

Email & Skype: info@chipsmall.com Web: www.chipsmall.com

Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China





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

User manual
UM EN FL MGUARD2

User manual

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

2013-07-17

Designation: UM EN FL MGuard2

Revision: 02

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 PCI4000		2701274
FL MGuard PCI4000 VPN		2701275
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 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.



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

Please observe the following notes

General terms and conditions of use for technical documentation

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

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

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

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	9
1.1	Device versions	11
2	Operating elements and LEDs	13
2.1	FL MGuard RS2000/4000	13
2.2	FL MGuard SMART2	14
2.3	FL MGuard PCI4000	15
2.4	FL MGuard DELTA TX/TX	16
3	Startup	17
3.1	Safety notes	17
3.2	Checking the scope of supply	19
3.3	Installing the FL MGuard RS4000/RS2000	20
3.3.1	Assembly/removal	20
3.3.2	Connecting to the network	20
3.3.3	Service contacts	21
3.3.4	Connecting the supply voltage	23
3.4	Connecting the FL MGuard SMART2	24
3.5	Installing the FL MGuard PCI4000	25
3.5.1	Installing the hardware	25
3.5.2	Power-over-PCI mode	26
3.6	Connecting the FL MGuard DELTA TX/TX	28
3.6.1	Connecting to the network	28
3.6.2	Connecting the supply voltage	28
4	Preparing the configuration	29
4.1	Connection requirements	29
4.2	Local configuration on startup (EIS)	30
4.2.1	Configuring the FL MGuard on startup with stealth mode by default ..	31
4.2.2	Configuring the FL MGuard on startup with router mode by default ..	36
4.2.3	Configuring the FL MGuard PCI4000 on startup	37
4.2.4	Configuring the FL MGuard PCI4000 on startup	41
4.3	Establishing a local configuration connection	43
4.4	Remote configuration	45
5	Configuration	47
5.1	Operation	47
5.2	Management menu	50
5.2.1	Management >> System Settings	50

5.2.2	Management >> Web Settings	68
5.2.3	Management >> Licensing	79
5.2.4	Management >> Update	82
5.2.5	Management >> Configuration Profiles	85
5.2.6	Management >> SNMP	89
5.2.7	Management >> Central Management	100
5.2.8	Management >> Restart	104
5.3	Network menu	104
5.3.1	Network >> Interfaces	104
5.3.2	Network >> NAT	142
5.3.3	Network >> DNS	147
5.3.4	Network >> DHCP	151
5.3.5	Network >> Proxy Settings	155
5.4	Authentication menu	156
5.4.1	Authentication >> Administrative Users	156
5.4.2	Authentication >> Firewall Users	159
5.4.3	Authentication >> RADIUS Servers	161
5.4.4	Authentication >> Certificates	163
5.5	Network Security menu	179
5.5.1	Network Security >> Packet Filter	179
5.5.2	Network Security >> DoS Protection	194
5.5.3	Network Security >> User Firewall	196
5.6	CIFS Integrity Monitoring menu	199
5.6.1	CIFS Integrity Monitoring >> Importable Shares	200
5.6.2	CIFS Integrity Monitoring >> CIFS Integrity Checking	201
5.6.3	CIFS Integrity Monitoring >> CIFS Integrity Status	207
5.6.4	CIFS Integrity Monitoring >> CIFS AV Scan Connector	210
5.7	IPsec VPN menu	214
5.7.1	IPsec VPN >> Global	214
5.7.2	IPsec VPN >> Connections	222
5.7.3	IPsec VPN >> L2TP over IPsec	251
5.7.4	IPsec VPN >> IPsec Status	252
5.8	SEC-Stick menu	253
5.8.1	Global	253
5.8.2	Connections	256
5.9	QoS menu	258
5.9.1	Ingress Filters	258
5.9.2	Egress Queues	261
5.9.3	Egress Queues (VPN)	263
5.9.4	Egress Rules	266
5.10	Redundancy	270
5.10.1	Redundancy >> Firewall Redundancy	270
5.10.2	Redundancy >> FW Redundancy Status	280
5.10.3	Ring/Network Coupling	285

5.11	Logging menu.....	286
5.11.1	Logging >> Settings	286
5.11.2	Logging >> Browse local logs	287
5.12	Support menu.....	291
5.12.1	Support >> Tools	291
5.12.2	Support >> Advanced	293
5.13	CIDR (Classless Inter-Domain Routing)	294
5.14	Network example diagram.....	295
6	Redundancy	297
6.1	Firewall redundancy	297
6.1.1	Components in firewall redundancy	298
6.1.2	Interaction of the firewall redundancy components	300
6.1.3	Firewall redundancy settings from previous versions	300
6.1.4	Requirements for firewall redundancy	300
6.1.5	Fail-over switching time	301
6.1.6	Error compensation through firewall redundancy	303
6.1.7	Handling firewall redundancy in extreme situations	304
6.1.8	Interaction with other devices	306
6.1.9	Transmission capacity with firewall redundancy	309
6.1.10	Limits of firewall redundancy	310
6.2	VPN redundancy	311
6.2.1	Components in VPN redundancy	311
6.2.2	Interaction of the VPN redundancy components	312
6.2.3	Error compensation through VPN redundancy	312
6.2.4	Setting the variables for VPN redundancy	313
6.2.5	Requirements for VPN redundancy	314
6.2.6	Handling VPN redundancy in extreme situations	314
6.2.7	Interaction with other devices	316
6.2.8	Transmission capacity with VPN redundancy	318
6.2.9	Limits of VPN redundancy	319
7	NOTE: Restart, recovery procedure, and flashing the firmware	323
7.1	Performing a restart.....	323
7.2	Performing a recovery procedure	324
7.3	Flashing the firmware/rescue procedure	325
7.3.1	Requirements for flashing	325
7.3.2	Flashing procedure for FL MGuard RS4000/RS2000, FL MGuard SMART2, FL MGuard DELTA TX/TX	326
7.3.3	Flashing procedure for the FL MGuard PCI4000	328
7.3.4	Installing the DHCP and TFTP server	329

8	Technical data	331
8.1	FL MGuard RS4000/RS2000	331
8.2	FL MGuard PCI4000.....	332
8.3	FL MGuard DELTA TX/TX.....	334
8.4	FL MGuard SMART2	335
8.5	Ordering data	336
8.5.1	Products	336
8.5.2	Accessories	336

1 Introduction

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

- Network card (FL MGUARD PCI4000)
- 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 the Phoenix Contact website at:
phoenixcontact.net/products

Network features

- Stealth (auto, static, multi), router (static, DHCP client), PPPoE (for DSL), PPTP (for DSL), and modem
- VLAN
- DHCP server/relay on the 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

- 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

FL MGuard

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 subjector
 - 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)
- Depending on the license: up to 250 VPN channels
- Hardware acceleration for encryption in the VPN

Additional features

- Remote logging
- Router/firewall redundancy (can be installed later for each license, not for firmware version 7.0))
- Administration using SNMP v1-v3 and FL MGuard device manager (FL MGuard DM)
- PKI support for HTTPS/SSH remote access
- Can act as an NTP and DNS server via the LAN interface

Support



Additional information on the device as well as on release **NOTE:** notes and software updates can be found on the Internet at: phoenixcontact.net/products.

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 RS4000/ FL MGuard RS2000

The **FL MGuard RS4000** is a security router 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 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)

TX/TX

Ethernet/Ethernet

TX/TX VPN

Ethernet/Ethernet + VPN

FL MGuard RS2000: (LAN/WAN)

TX/TX VPN

Ethernet/Ethernet + VPN



Figure 1-1 FL MGuard RS4000/FL MGuard RS2000

FL MGuard

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.

The **FL MGuard SMART2** is a further development of the **FL MGuard SMART**.



Figure 1-2 FL MGuard SMART2

FL MGuard PCI4000

The FL MGuard PCI4000 has the design of a PCI-compatible plug-in board.

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 1-3 FL MGuard PCI4000

FL MGuard DELTA TX/TX

The **FL MGuard DELTA TX/TX** is ideal for use in desktop applications, in distribution compartments, and other environments close to production process 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 1-4 FL MGuard DELTA TX/TX

2 Operating elements and LEDs

2.1 FL MGuard RS2000/4000

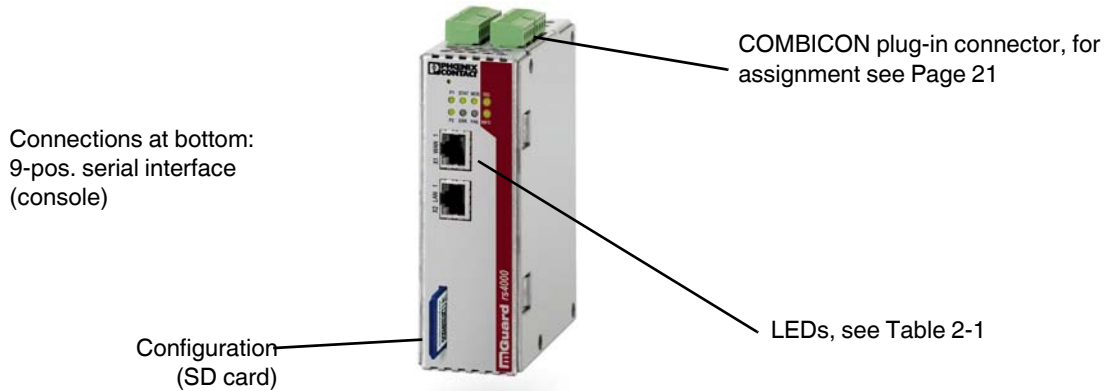


Figure 2-1 Operating elements and LEDs on the FL MGuard RS2000/4000

Table 2-1 LEDs on the FL MGuard RS2000/4000

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. <ul style="list-style-type: none"> – 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 <i>recovery procedure</i> (see Page 324) 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 alarm output is open due to an error (see “Installing the FL MGuard RS4000/RS2000” on page 20). (The alarm output is interrupted during a restart.)
MOD	Green	ON	Connection via modem established
INFO	Green	ON	The configured VPN connection has been established.
		Flashing	The configured VPN connection is being established or aborted.
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	

2.2 FL MGuard SMART2



Figure 2-2 Operating elements and LEDs on the FL MGuard SMART2

Table 2-2 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. <ul style="list-style-type: none"> 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 <i>recovery procedure</i> (see “Performing a recovery procedure” on page 324) 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 Rescue button. See “NOTE: Restart, recovery procedure, and flashing the firmware” on page 323

2.3 FL MGuard PCI4000

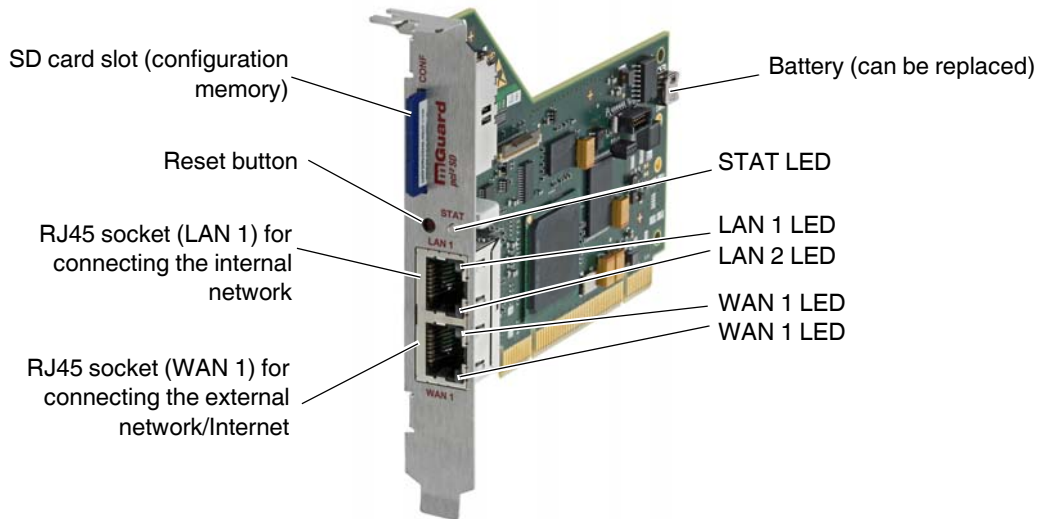


Figure 2-3 Operating elements and LEDs on the FL MGuard PCI4000

Table 2-3 LEDs on the FL MGuard PCI4000 SD

LEDs	State		Meaning
WAN 1 LAN 1	Green	ON	Full duplex
		OFF	Half duplex
WAN 2 LAN 2	Yellow	ON	10 Mbps
		Flashing	10 Mbps, data transmission active
	Green	ON	100 Mbps
		Flashing	100 Mbps, data transmission active
LAN 1 LAN 2 WAN 1	Various LED light codes		Recovery procedure/flashing See “NOTE: Restart, recovery procedure, and flashing the firmware” on page 323
STAT	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 FL MGuard is connected correctly and ready to operate.
	Red	Flashing	System error. Restart the device. <ul style="list-style-type: none"> 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 <i>recovery procedure</i> (see “Performing a recovery procedure” on page 324) or contact your dealer.

2.4 FL MGUARD DELTA TX/TX

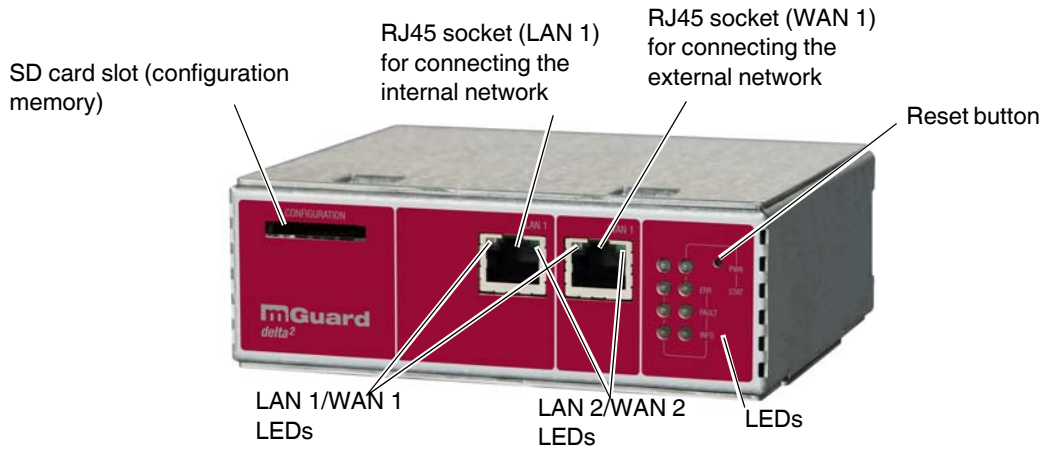


Figure 2-4 Operating elements and LEDs on the

Table 2-4 LEDs on the FL MGUARD DELTA TX/TX

LEDs	State		Meaning
WAN 1 LAN 1	Green	ON	Full duplex
		OFF	Half duplex
WAN 2 LAN 2	Yellow	ON	10 Mbps
		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 FL MGUARD is ready to operate.
ERR	Red	ON	System error
FAULT	Red	ON	FL MGUARD in the booting or flashing state
INFO			Not used

3 Startup

3.1 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 sockets**

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

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

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 the connecting cable. Only use the network connector for connection to a network.

**NOTE: Select suitable ambient conditions**

- Ambient temperature:
 - 0°C ... +40°C (FL MGuard SMART2, FL MGuard DELTA TX/TX)
 - 0°C ... +60°C (FL MGuard PCI4000 with battery)
 - 0°C ... +70°C (FL MGuard PCI4000 without battery)
 - 20°C ... +60°C (FL MGuard RS4000/FL MGuard RS2000)
- Maximum humidity, non-condensing
 - 20% ... 90% (FL MGuard SMART2)
 - 5% ... 95%, (FL MGuard RS4000/FL MGuard RS2000, FL MGuard PCI4000, 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:

Step	Aim	Page
1	Check the scope of supply Read the release notes	Page 19
2	Connect the device	
	FL MGuard RS4000/FL MGuard RS2000	Page 20
	FL MGuard PCI4000	Page 25
	FL MGuard DELTA TX/TX	Page 28
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	Page 30

3.2 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 RS4000, FL MGuard RS2000, FL MGuard SMART2, FL MGuard PCI4000, FL MGuard DELTA TX/TX device
- Packing slip

The FL MGuard RS4000 and FL MGuard RS2000 also include:

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

The FL MGuard DELTA TX/TX also includes:

- 12 V DC power supply including different country adapters

3.3 Installing the FL MGuard RS4000/RS2000

3.3.1 Assembly/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.

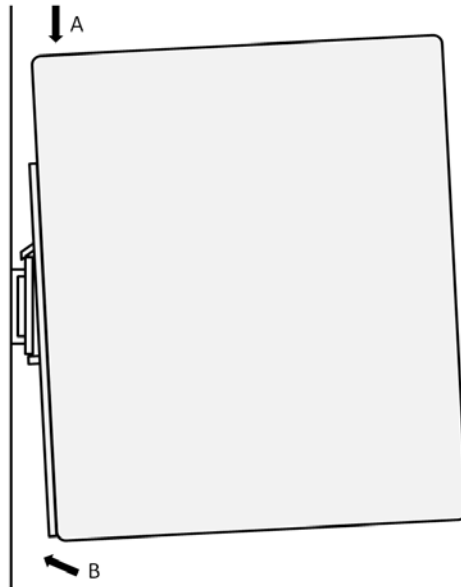


Figure 3-1 Mounting the FL MGuard RS4000/RS2000 on a DIN rail

- 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.

3.3.2 Connecting to the network



WARNING: Only connect the FL MGuard network ports to LAN installations. Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets 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).

3.3.3 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 and 7.5. The “Service 2” contacts shall be made available with a later firmware version.



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

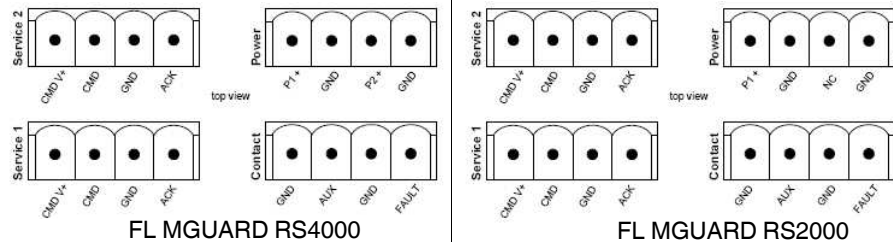


Table 3-1

Service 2	CMD V+	CMD	GND	ACK	<table border="1"> <thead> <tr> <th>Power</th> <th>P1+</th> <th>GND</th> <th>P2+</th> <th>GND</th> </tr> </thead> <tbody> <tr> <td></td> <td>+24 V</td> <td>+0 V</td> <td>+24 V</td> <td>+0 V</td> </tr> <tr> <td></td> <td colspan="2">See Section 3.3.4</td> <td colspan="2">FL MGuard RS4000 only, see Section 3.3.4</td> </tr> <tr> <td rowspan="2">Service 1</td> <td>CMD V+</td> <td>CMD</td> <td>GND</td> <td>ACK</td> <td rowspan="2"> <table border="1"> <thead> <tr> <th>Contact</th> <th>GND</th> <th>AUX</th> <th>GND</th> <th>FAULT</th> </tr> </thead> <tbody> <tr> <td></td> <td>Not used</td> <td>Not used</td> <td>Alarm output (-)</td> <td>Alarm output (+)¹</td> </tr> <tr> <td></td> <td colspan="2">Example</td> <td colspan="2">Example</td> </tr> </tbody> </table> </td> </tr> <tr> <td></td> <td>Not used</td> <td>Not used</td> <td>Not used</td> <td>Not used</td> </tr> <tr> <td></td> <td>External control switch, pin 1</td> <td>External control switch, pin 2</td> <td>Alarm output (-)</td> <td>Alarm output (+)</td> </tr> <tr> <td></td> <td colspan="2">Example</td> <td colspan="2">Example</td> </tr> </tbody> </table>	Power	P1+	GND	P2+	GND		+24 V	+0 V	+24 V	+0 V		See Section 3.3.4		FL MGuard RS4000 only, see Section 3.3.4		Service 1	CMD V+	CMD	GND	ACK	<table border="1"> <thead> <tr> <th>Contact</th> <th>GND</th> <th>AUX</th> <th>GND</th> <th>FAULT</th> </tr> </thead> <tbody> <tr> <td></td> <td>Not used</td> <td>Not used</td> <td>Alarm output (-)</td> <td>Alarm output (+)¹</td> </tr> <tr> <td></td> <td colspan="2">Example</td> <td colspan="2">Example</td> </tr> </tbody> </table>	Contact	GND	AUX	GND	FAULT		Not used	Not used	Alarm output (-)	Alarm output (+) ¹		Example		Example			Not used	Not used	Not used	Not used		External control switch, pin 1	External control switch, pin 2	Alarm output (-)	Alarm output (+)		Example		Example	
	Power	P1+	GND	P2+		GND																																																		
	+24 V	+0 V	+24 V	+0 V																																																				
	See Section 3.3.4		FL MGuard RS4000 only, see Section 3.3.4																																																					
Service 1	CMD V+	CMD	GND	ACK	<table border="1"> <thead> <tr> <th>Contact</th> <th>GND</th> <th>AUX</th> <th>GND</th> <th>FAULT</th> </tr> </thead> <tbody> <tr> <td></td> <td>Not used</td> <td>Not used</td> <td>Alarm output (-)</td> <td>Alarm output (+)¹</td> </tr> <tr> <td></td> <td colspan="2">Example</td> <td colspan="2">Example</td> </tr> </tbody> </table>	Contact	GND	AUX	GND	FAULT		Not used	Not used	Alarm output (-)	Alarm output (+) ¹		Example		Example																																					
	Contact	GND	AUX	GND		FAULT																																																		
	Not used	Not used	Alarm output (-)	Alarm output (+) ¹																																																				
	Example		Example																																																					
	Not used	Not used	Not used	Not used																																																				
	External control switch, pin 1	External control switch, pin 2	Alarm output (-)	Alarm output (+)																																																				
	Example		Example																																																					

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

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

A standard lamp (24 V) can be connected between **contacts GND (-) and ACK (+)**. The contact is continuously 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 214 under “Options”).

Product designation

Operating a connected button

- To establish the VPN connection, hold down the button for a few seconds until the signal output flashes. Only 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. Only 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.

ACK 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 ACK LED is ON, the VPN connection is present.

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

Signal contact (alarm output)

The signal contact monitors the function of the FL MGuard RS4000/RS2000 and thus enables remote diagnostics. 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 set (see “Signal Contact” on page 52).
- 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 configuration” in the software configuration.

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 COMBICON plug-in connector, which is located on the top of the device.



When the COMBICON connector is removed or inserted during operation of the FL MGUARD, the FL MGUARD is directly switched off.

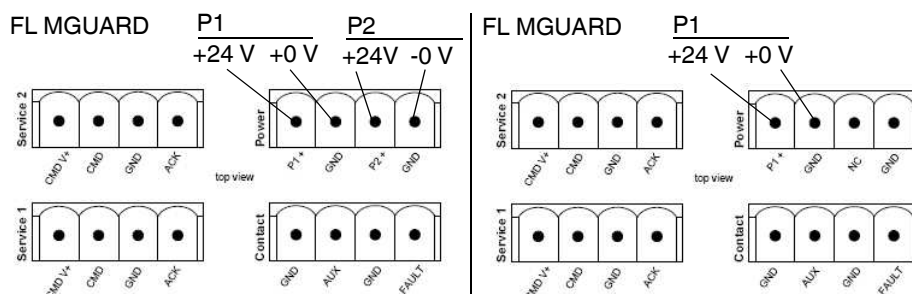


Figure 3-2 Connecting the supply voltage: FL MGUARD RS4000/FL MGUARD RS2000

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

- Take off the COMBICON connectors for the power supply and the service contacts.
- Do not connect the service contacts to an external voltage source.
- Wire the supply voltage lines to the corresponding COMBICON connector (P1/P2) of the FL MGUARD. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the COMBICON connectors in the intended COMBICON sockets on the top of the FL MGUARD (see Figure 3-2).

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

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

Redundant power 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 (P1/P2) or by installing an appropriate wire bridge between connections P1 and P2.

3.4 Connecting the FL MGUARD SMART2



LAN port

Ethernet connector for direct connection to the device or network to be protected (**local** device or network).

USB connector

For connection to the USB interface of a computer.

For the power supply (default settings).

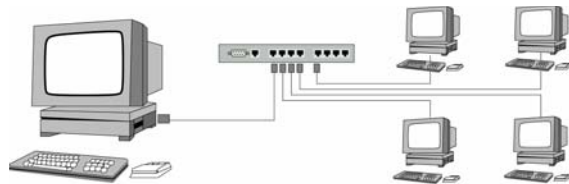
The FL MGUARD SMART2 (not the FL MGUARD SMART) can be configured such that a serial console is available via the USB connector (see Section 5.3.1.5).

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.)

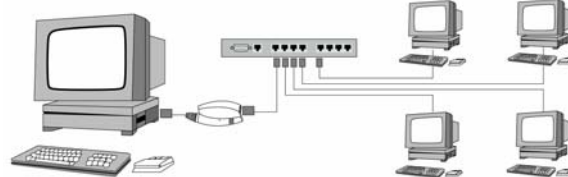


Figure 3-3 FL MGUARD SMART2: Connection to the network.



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, and the operator may be required to take appropriate measures.

3.5 Installing the FL MGUARD PCI4000



WARNING: This is a Class A item of equipment. This equipment can cause radio interference in residential areas, and the operator may be required to take 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.

3.5.1 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

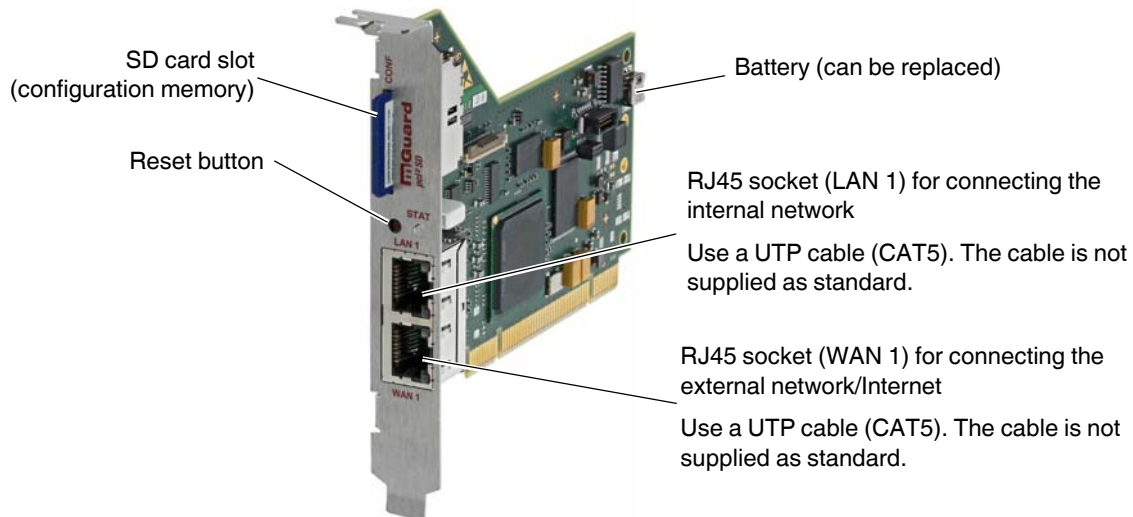


Figure 3-4 FL MGUARD PCI4000 structure

Install the FL MGUARD PCI4000 in a free PCI slot. Observe the notes in the documentation for your system.