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

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 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.

$\mathbf{i}$ | 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

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)
	–	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

> **i**   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)		**FL MGUARD RS2000: (LAN/WAN)**	
TX/TX	Ethernet/Ethernet	TX/TX VPN	Ethernet/Ethernet + VPN
TX/TX VPN	Ethernet/Ethernet + VPN		

Figure 1-1   FL MGUARD RS4000/FL MGUARD RS2000

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

COMBICON plug-in connector, for assignment see Page 21

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

LEDs, see Table 2-1

Configuration (SD card)
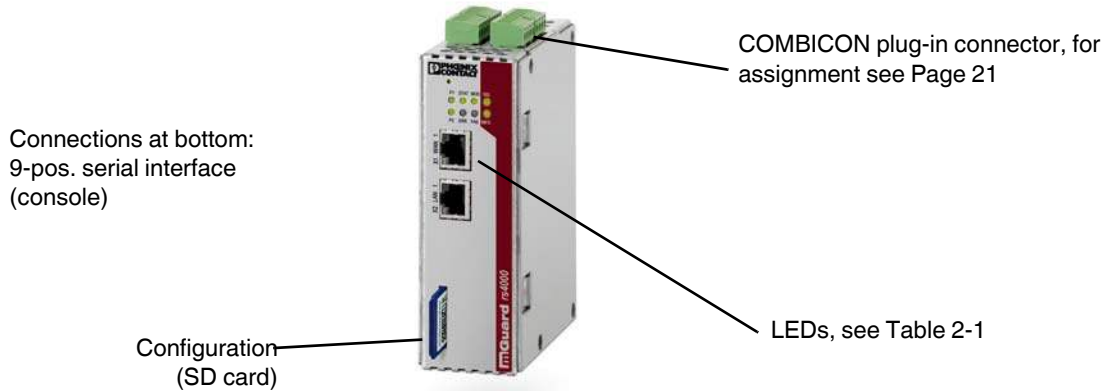
Figure 2-1   Operating elements and LEDs on the FL MGUARD RS2000/4000

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. – 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 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)
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 FL MGUARD SMART2

Rescue button

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

LED 1   LED 2   LED 3

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. • 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 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
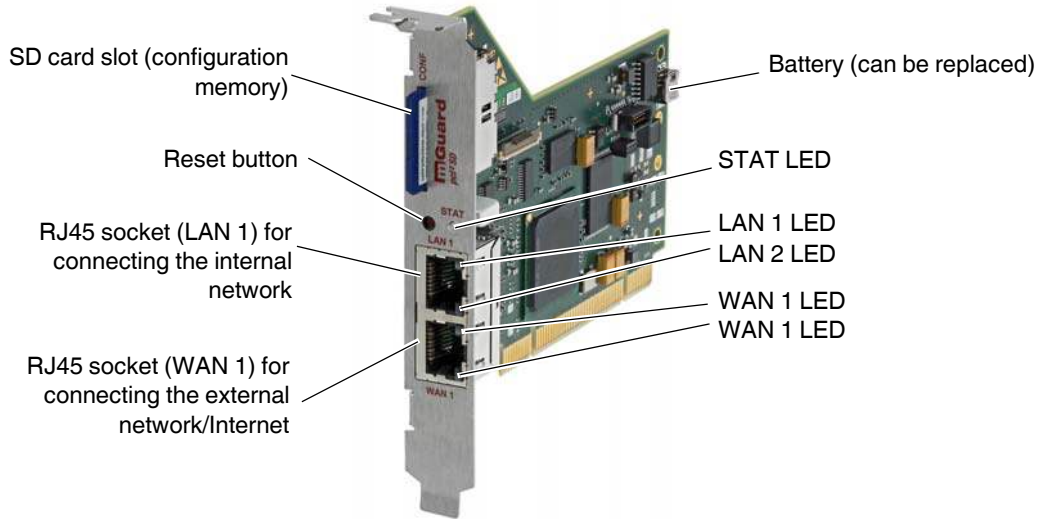
Figure 2-3   Operating elements and LEDs on the FL MGUARD PCI4000

Table 2-3   LEDs on the FL MGUARD PCI4000 SD

LEDs	State		Meaning
WAN 1	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
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. • 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 324) or contact your dealer.

2.4 FL MGUARD DELTA TX/TX

SD card slot (configuration memory)

RJ45 socket (LAN 1) for connecting the internal network

RJ45 socket (WAN 1) for connecting the external network

Reset button

LAN 1/WAN 1 LEDs

LAN 2/WAN 2 LEDs
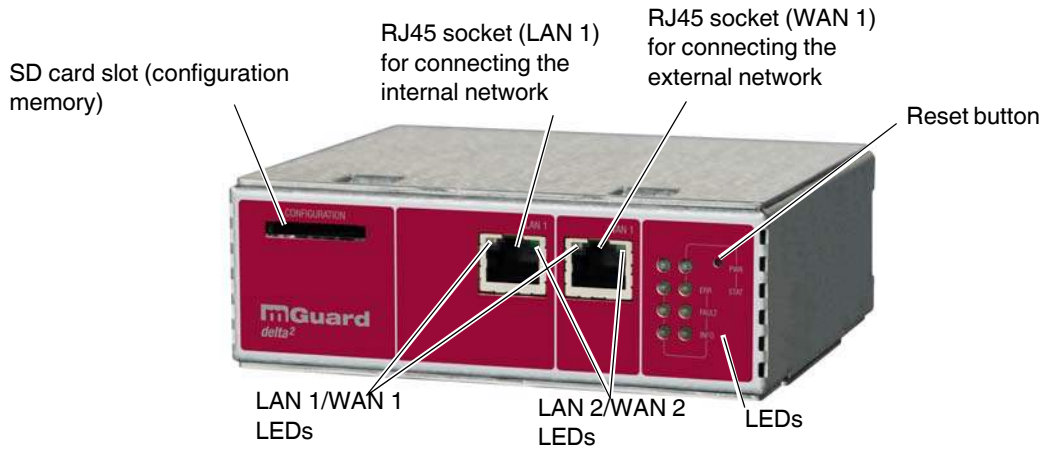
LEDs

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	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 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	Page 19
	Read the release notes	
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.	Page 30
	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	

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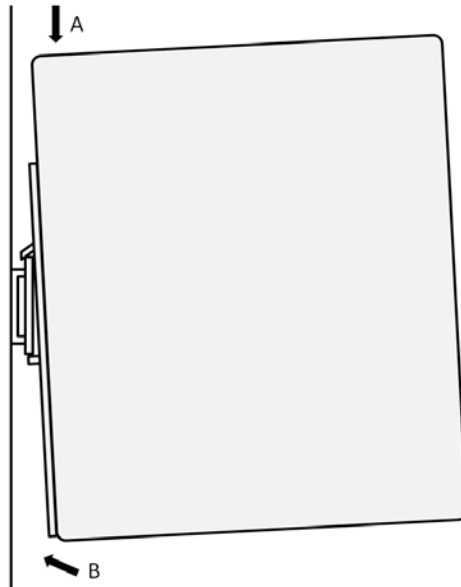
Figure 3-1   Mounting the FL MGUARD RS4000/RS2000 on a DIN rail

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

FL MGUARD RS4000   FL MGUARD RS2000
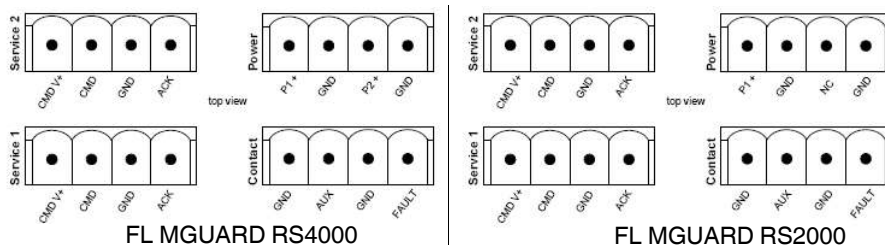
Table 3-1

Service 2	CMD V+	CMD	GND	ACK
	Not used	Not used	Not used	Not used

Service 1	CMD V+	CMD	GND	ACK
	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	

Contact	GND	AUX	GND	FAULT
	Not used	Not used	Alarm output (-)	Alarm output (+)[1]
				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").

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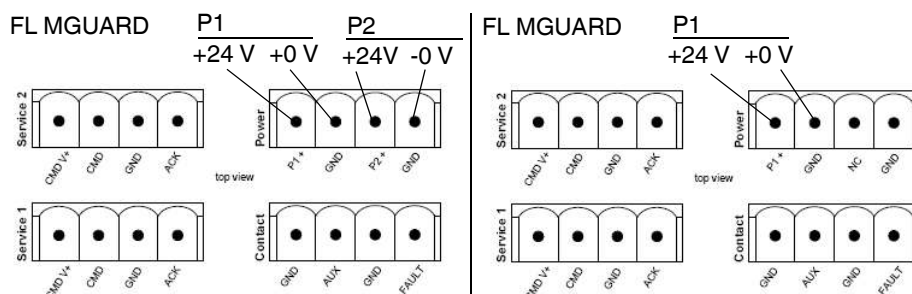
Figure 3-2   Connecting the supply voltage: FL MGUARD RS4000/FL MGUARD RS2000

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:
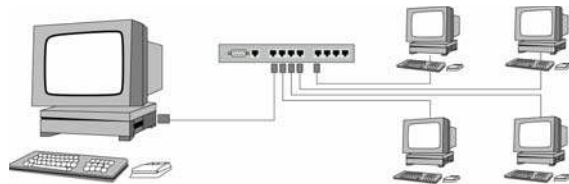
After:

(A LAN can also be on the left.)
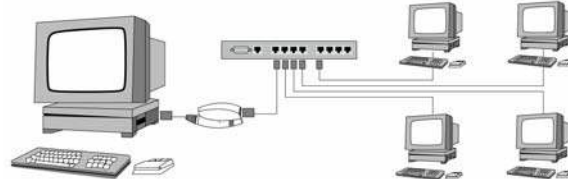
Figure 3-3   FL MGUARD SMART2: Connection to the network**.**

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

SD card slot (configuration memory)

Reset button

Battery (can be replaced)

RJ45 socket (LAN 1) for connecting the internal network

Use a UTP cable (CAT5). The cable is not supplied as standard.

RJ45 socket (WAN 1) for connecting the external network/Internet

Use a UTP cable (CAT5). The cable is not supplied as standard.
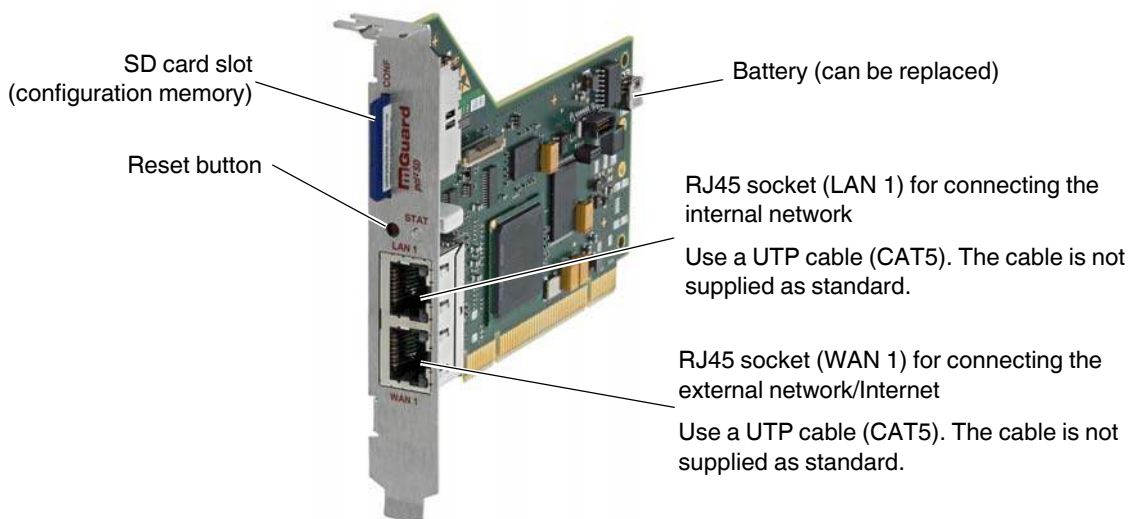
Figure 3-4   FL MGUARD PCI4000 structure

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

3.5.2 Power-over-PCI mode

Stealth mode in power-over-PCI mode
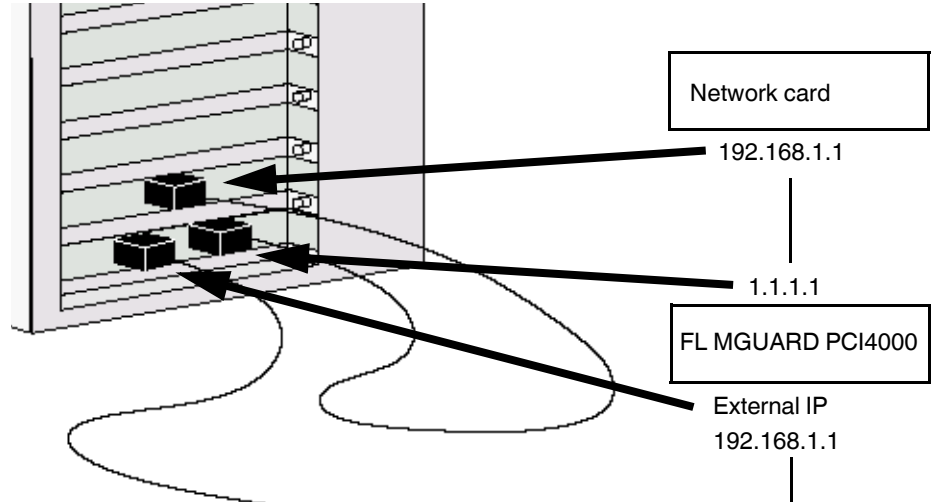
Figure 3-5   Power-over-PCI mode: stealth mode

A previously installed network card is connected to the LAN port of the
FL MGUARD PCI4000, which is located in the same computer or in another computer (see
"Connecting the FL MGUARD DELTA TX/TX" on page 28).

In *stealth* mode, the IP address configured for the network interface of the operating system
(LAN port) is also used by the FL MGUARD for its WAN port. This means that the
FL MGUARD does not appear as a separate device with its own address for data traffic to
and from the computer.

In stealth mode, PPPoE and PPTP cannot be used.

Router mode in power-over-PCI mode
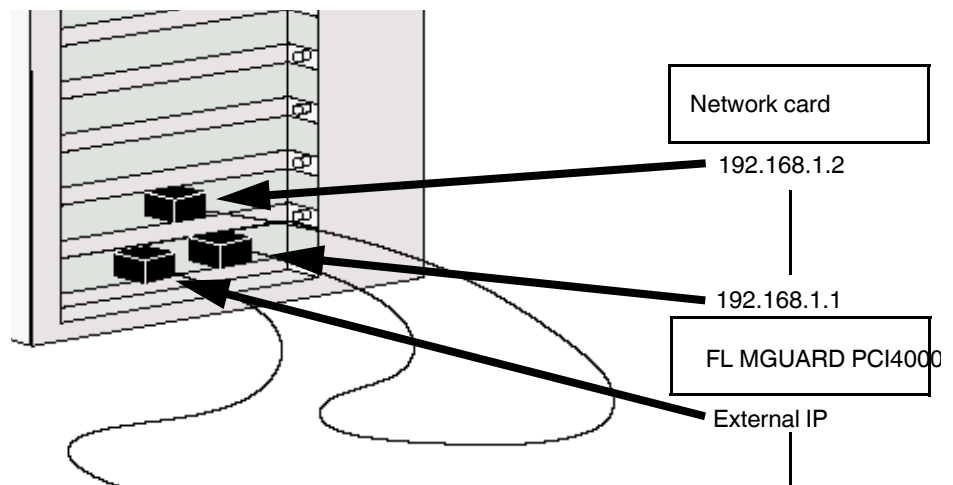
Figure 3-6   Power-over-PCI mode: router mode

If the FL MGUARD is in *router* mode (or *PPPoE* or *PPTP* mode), the FL MGUARD and the network card connected to its LAN socket – installed in the same computer or another computer – act as a separate network.

For the IP configuration of the network interface of the operating system for the computer in which the network card is installed, this means that an IP address must be assigned to this network interface that differs from the internal IP address of the FL MGUARD (by default upon delivery this is 192.168.1.1).

A third IP address is used for the interface of the FL MGUARD to the WAN. It is used for connection to an external network (e.g., Internet).

3.6 Connecting the FL MGUARD DELTA TX/TX

> **NOTE: Notes on mounting and installation**
>
> Only connect the RJ45 Ethernet ports of the FL MGUARD to matching network installations. Some telecommunications connections also use RJ45 sockets. These must not be connected to the RJ45 ports of the FL MGUARD.
>
> 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.

3.6.1 Connecting to the network

- 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).

3.6.2 Connecting the supply voltage

- Connect the wide-range power supply unit of the FL MGUARD to a suitable power supply. Connect the low-voltage connector of the power supply unit on the back of the FL MGUARD.

Figure 3-7   Low-voltage connector of the power supply unit

The status LED PWR lights up green when the supply voltage has been connected properly.

The FL MGUARD boots the firmware. The status LED STAT flashes green.

The FL MGUARD is ready for operation as soon as the LAN/WAN Ethernet socket LEDs light up.

Additionally, the status LED PWR lights up green and the status LED STAT flashes green at heartbeat.

4 Preparing the configuration

4.1 Connection requirements

FL MGUARD RS4000/RS2000

– 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 FL MGUARD.
– **For remote configuration**: The FL MGUARD must be configured so that remote configuration is permitted.
– The FL MGUARD must be connected, i.e., the required connections must be working.

FL MGUARD PCI4000

– For local configuration: The computer used for configuration must meet the following requirements:
  – The computer must be connected to the FL MGUARD via its LAN connection or via the local network.
– For remote configuration: The FL MGUARD must be configured so that remote configuration is permitted.
– The FL MGUARD must be connected, i.e. ,the required connections must be working. **The FL MGUARD must** be connected, i.e., the required connections must be working.

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 FL MGUARD.
– **For remote configuration**: The FL MGUARD must be configured so that remote configuration is permitted.
– The FL MGUARD must be connected, i.e., the required connections must be working.

4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of FL MGUARD products provided in stealth mode is considerably easier. From this version onwards, the EIS (**E**asy **I**nitial **S**etup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The FL MGUARD is configured using a web browser on the computer used for configuration (e.g., MS Internet Explorer Version 8 or later, Mozilla Firefox Version 3.6 or later, Google Chrome or Apple Safari).

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

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

Table 4-1   Preset addresses

Default settings	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000/RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

FL MGUARDs provided in stealth network mode are preset to the "multiple clients" stealth configuration. In this mode, you need to configure a management IP address and default gateway if you want to use VPN connections (see page 114). Alternatively, you can select a different stealth configuration than the "multiple clients" configuration or use another network mode.

The configuration on startup is described in two sections:

– For devices provided in the "stealth" network mode, in Section 4.2.1 from page 31
– For devices provided in the "router" network mode, in Section 4.2.2 on page 36

4.2.1 Configuring the FL MGUARD on startup with stealth mode by default

On initial startup of devices provided in stealth mode, the FL MGUARD can be accessed via two addresses:

– https://192.168.1.1/ (see page 31)
– https://1.1.1.1/ (see page 32)

Alternatively, an IP address can be assigned via BootP (e.g., using IPAssign.exe) (see "Assigning the IP address via BootP" on page 33).

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

Computers can access the FL MGUARD via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the FL MGUARD. For this purpose, the FL MGUARD 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.

> **i** – 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.

> **i** For the **FL MGUARD PCI4000**, the startup procedure differs from the one described here.
>
> For initial configuration of the
> – FL MGUARD PCI4000, please refer to "Configuring the FL MGUARD PCI4000 on startup" on page 37.

4.2.1.1 IP address 192.168.1.1

> **i** For devices provided in stealth mode, the FL MGUARD 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 FL MGUARD is in the delivery state.
> – The FL MGUARD was reset to the default settings via the web interface (see"Configuration Profiles" on page 85) and restarted.
> – The rescue procedure (flashing of the FL MGUARD) or the recovery procedure have been performed (see Section 7).

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

Under **Windows XP**, proceed as follows:
• Click on "Start, Control Panel, Network Connections".
• Right-click on the LAN adapter icon to open the context menu.
• In the context menu, click on "Properties".
• In the "Properties of local network LAN connections" dialog box, select the "General" tab.
• Under "This connection uses the following items", select "Internet Protocol (TCP/IP)".

• Then click on "Properties" to display the following dialog box:

Figure 4-1   Internet Protocol (TCP/IP) Properties

• First select "Use the following IP address", then enter the following addresses, for example:

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

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

4.2.1.2   IP address https://1.1.1.1/

With a configured network interface

In order for the FL MGUARD 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 (see Figure 3-3 on page 24) and if the default gateway can be accessed via the WAN port of the FL MGUARD at the same time.

In this case, the web browser establishes a connection to the FL MGUARD configuration interface after address https://1.1.1.1/ is entered (see "Establishing a local configuration connection" on page 43). Continue from this point.

i	After access via IP address 1.1.1.1, the FL MGUARD can no longer be accessed via IP address 192.168.1.1

4.2.1.3   Assigning the IP address via BootP

i

> 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 FL MGUARD 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.

This section explains IP address assignment using the "IP Assignment Tool" Windows software (IPAssign.exe). This software can be downloaded free of charge at phoenixcontact.net/catalog or at www.innominate.com under "Downloads > Software".

Notes for BootP

During initial startup, the FL MGUARD transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the FL MGUARD 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 FL MGUARD no longer sends BootP requests, not even after it has been restarted. For the FL MGUARD 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

Requirements

The FL MGUARD is connected to a computer using a Microsoft Windows operating system.

IP address assignment using IPAssign.exe

Step 1: downloading and executing the program

• On the Internet, select the link phoenixcontact.net/catalog.
• Enter order number 2701094 in the search field, for example.

The BootP IP addressing tool can be found under "Configuration file".

• Double-click on the "IPAssign.exe" file.
• In the window that opens, click on "Run".

Step 2: "IP Assignment Wizard"

The program opens and the start screen of the addressing tool appears.

The program is mostly in English for international purposes. 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 FL MGUARD in the following 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.
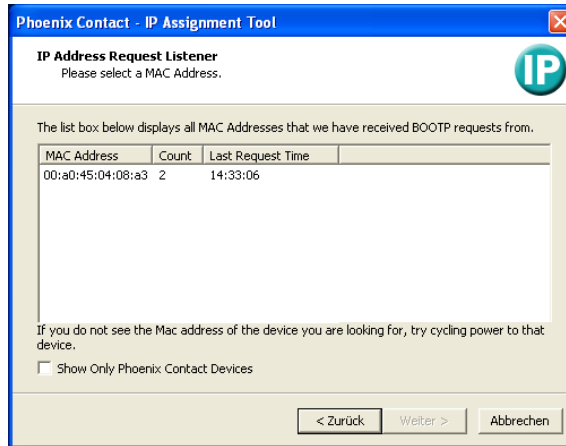
Figure 4-2   "IP Address Request Listener" window

In this example, the FL 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
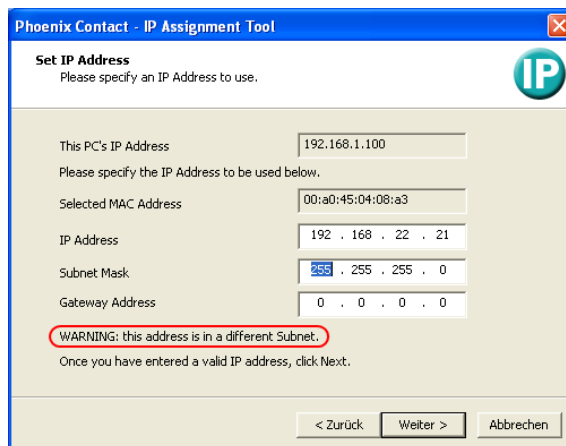
Figure 4-3   "Set IP Address" window with incorrect settings

• 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 FL MGUARD.
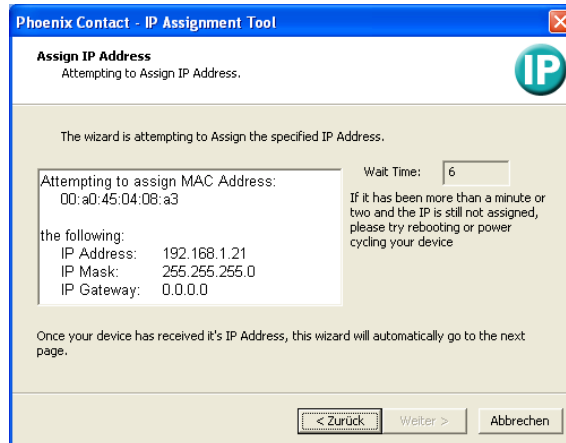
Figure 4-4   "Assign IP Address" window

Following successful transmission, the next window opens.

Step 6: finishing IP address assignment

The window that opens informs you that IP 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 FL MGUARD web interface under Network >> Interfaces (see page 104). |

4.2.2 Configuring the FL MGUARD on startup with router mode by default

i	By default upon delivery, following reset to the default settings or after flashing the FL MGUARD, the FL MGUARD can be accessed within the network 192.168.1.0/24 via the LAN interface (LAN interfaces 4 to 7 for the FL MGUARD DELTA TX/TX) 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 XP**, proceed as follows:
• Click on "Start, Control Panel, Network Connections".
• Right-click on the LAN adapter icon to open the context menu.
• In the context menu, click on "Properties".
• In the "Properties of local network LAN connections" dialog box, select the "General" tab.
• Under "This connection uses the following items", select "Internet Protocol (TCP/IP)".
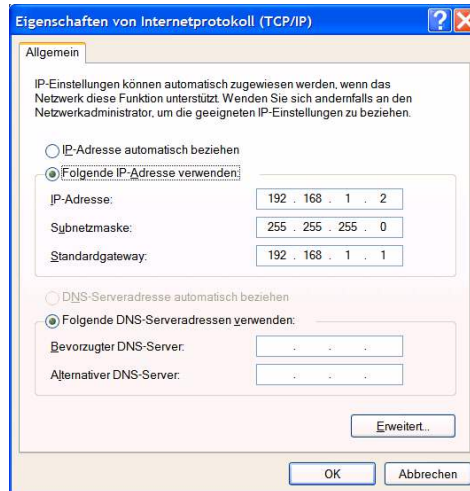• Then click on "Properties" to display the following dialog box:
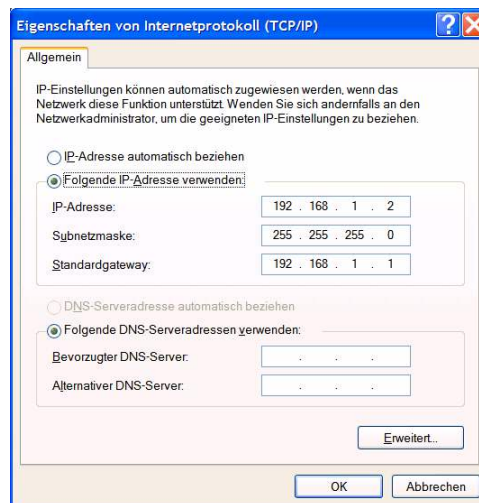
Figure 4-5   Internet Protocol (TCP/IP) Properties

• First select "Use the following IP address", then enter the following addresses, for example:

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

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

4.2.3 Configuring the FL MGUARD PCI4000 on startup

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

4.2.3.1 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 FL MGUARD boots the firmware. The STAT status LED flashes green during this time.

The FL MGUARD 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 FL MGUARD is configured using a web browser (e.g., MS Internet Explorer Version 8 or later, Mozilla Firefox Version 3.6 or later, Google Chrome or Apple Safari) on the locally connected computer.

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

The FL MGUARD 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 4.2.3.2).

A security message indicating a possible invalid/not trusted certificate is displayed. This message results from the use of an FL 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.
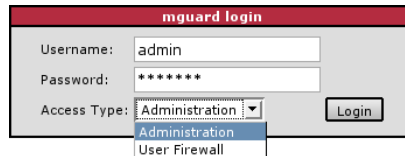
Figure 4-6   Login

• Select "Administration" as the access and enter your user name and password.

The following is set by default for administration (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 FL MGUARD user interface (see "Configuration" on page 47).

> **ⓘ** For security reasons, we recommend you change the default root and administrator passwords during initial configuration (see "Authentication >> Administrative Users" on page 156).

4.2.3.2 Start up the FL MGUARD PCI4000 via a temporary management IP address

If the 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.

> **i** 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.

Start 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 FL MGUARD 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 FL MGUARD as described in "Configuring the FL MGUARD PCI4000" on page 38.

4.2.3.3   Start up the 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/catalog or at www.innominate.com under "Downloads > Software".

| | IP address assignment using IPAssign is described in detail in "Assigning the IP address via BootP" on page 33. |

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 immediately accessed under these parameters.

• Enter the addressed assigned via BootP in the browser: e.g., https://192.168.1.1/

Configure the FL MGUARD as described in "Configuring the FL MGUARD PCI4000" on page 38.

4.2.4 Configuring the FL MGUARD PCI4000 on startup

Installing the PCI card

- If the PCI card has not yet been installed in your computer, first proceed as described under "Connecting the FL MGUARD DELTA TX/TX" on page 28.

-

Configuring the network interface

If the FL MGUARD

– Is operated in **power-over-PCI mode** and the network interface of the computer that is connected to the LAN interface of the FL MGUARD has not yet been configured

This network interface must be configured before the FL MGUARD can be configured.

Under **Windows XP**, proceed as follows to configure the network interface:

- Click on "Start, Control Panel, Network Connections".
- Right-click on the LAN adapter icon to open the context menu. In the context menu, click on "Properties".
- In the "Properties of local network LAN connections" dialog box, select the "General" tab.
- Under "This connection uses the following items", select "Internet Protocol (TCP/IP)".
- Then click on "Properties" to display the following dialog box:
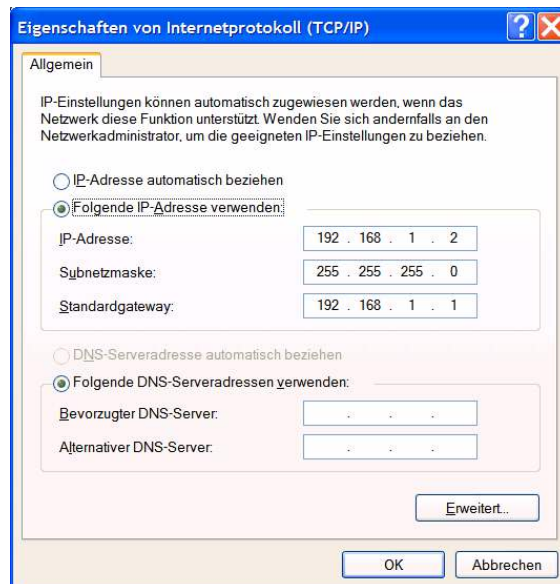
Figure 4-7   Internet Protocol (TCP/IP) Properties

Default gateway

Once you have configured the network interface, it should be possible to access the configuration interface of the FL MGUARD using a web browser under the URL "https://1.1.1.1/".

If this is not possible, the default gateway of your computer probably cannot be accessed. In this case, your computer should be simulated as follows:

Initializing the default gateway

Determine the currently valid default gateway address.
- Under **Windows XP**, carry out the steps described under "Configuring the network interface" on page 41 to open the "Internet Protocol (TCP/IP) Properties" dialog box.
- If no IP address has been specified for the default gateway in this dialog box (e.g., because "Obtain an IP address automatically" has been activated), then enter the IP address manually.

  To do so, first select "Use the following IP address", then enter the following addresses, for example:

IP address:	192.168.1.2	Do not under any circumstances assign an address such as 1.1.1.2 to the configuration computer.
Subnet mask:	255.255.255.0	
Default gateway:	192.168.1.1	

- In DOS (Start, Programs, Accessories, Command Prompt), enter the following:
  arp -s <IP address of the default gateway> 00-aa-aa-aa-aa-aa
  Example:
  You have determined or specified the address of the default gateway as: 192.168.1.1. The command should then be:
  arp -s 192.168.1.1 00-aa-aa-aa-aa-aa
- To proceed with the configuration, establish the configuration connection (see "Establishing a local configuration connection" on page 43).
- After configuration, reset the default gateway. To do this, either restart the configuration computer or enter the following command in DOS:
  arp -d

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

4.3   Establishing a local configuration connection

Web-based administrator interface

The FL MGUARD is configured via a web browser (e.g., Mozilla Firefox, MS Internet Explorer, Google Chrome, or Apple Safari) that is executed on the configuration computer.

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

Depending on the model, the FL MGUARD is set to *stealth* or *router* network mode by default upon delivery and can be accessed accordingly using the following addresses:

Table 4-2   Preset addresses

Default settings	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000/RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

*   Start a web browser.

    (For example: Mozilla Firefox, MS Internet Explorer, Google Chrome, or Apple Safari; the web browser must support SSL encryption (i.e., HTTPS).)

*   Make sure that the browser does not automatically dial a connection when it is started as this could make it more difficult to establish a connection to the FL MGUARD.

In **MS 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".
*   In the address line of the web browser, enter the full address of the FL MGUARD (see Table 4-2).

The administrator web page of the FL MGUARD can then be accessed.

If the administrator web page of the FL MGUARD cannot be accessed

If you have forgotten the configured address

If the address of the FL MGUARD in *router*, *PPPoE* or *PPTP* mode has been set to a different value and the current address is not known, the FL MGUARD must be reset to the default settings specified above for the IP address of the FL MGUARD using the **Recovery** procedure (see "Performing a recovery procedure" on page 324).

If the administrator web pate 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 30).
*   Disable any active firewalls.
*   Make sure that the browser does not use a proxy server.

    In **MS 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 a successful connection establishment

Once a connection has been established successfully, the following security alert is displayed (MS Internet Explorer):
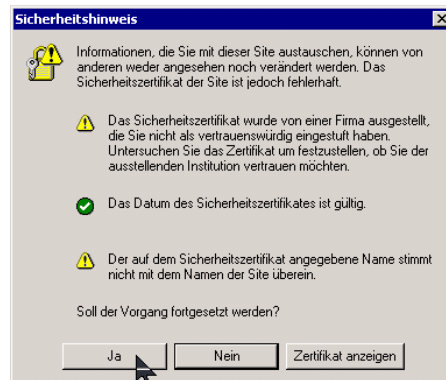
Figure 4-8   Security alert

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.
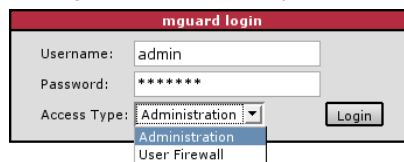
Figure 4-9   Login

 The "User Firewall" access type is **not** available on the **FL MGUARD RS2000.**

• Select the access type – Administration or User Firewall – and enter your user name and password which are specified for this access type. (For user firewall, see "Network Security >> User Firewall" on page 196.)

The following is set by default for administration (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 FL MGUARD user interface (see "Configuration" on page 47).

i | For security reasons, we recommend you change the default root and administrator passwords during initial configuration (see "Authentication >> Administrative Users" on page 156).

4.4 Remote configuration

Requirement

The FL MGUARD must be configured so that remote configuration is permitted.

The option for remote configuration is disabled by default.

To enable remote configuration (see "Management >> Web Settings" on page 68 and "Access" on page 69) proceed as follows.

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer (e.g., Mozilla Firefox, MS Internet Explorer, Google Chrome, or Apple Safari; the web browser must support HTTPS).
- Under address, enter the IP address where the FL MGUARD can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If this FL MGUARD can be accessed over the Internet 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 partner: 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

- To configure the device, make the desired or necessary settings on the individual pages of the FL MGUARD user interface (see "Configuration" on page 47).

5 Configuration

5.1 Operation

You can click on the desired configuration via the menu on the left-hand side, e.g., "Management, Licensing".

The page is then displayed in the main window – usually in the form of one or more tab pages – where settings can be made. If the page is organized into several tab pages, you can switch between them using the *tabs* at the top.

Working with tab pages

– You can make the desired entries on the corresponding tab page (see also "Working with sortable tables" on page 47).

– To apply the settings on the device, you must click on the **Apply** button.

Once the settings have been applied by the system, a confirmation message appears. This indicates that the new settings have taken effect. They also remain valid after a restart (reset).

– You can return to the previously accessed page by clicking on the **Back** button located at the bottom right of the page, if available.

Entry of impermissible values

If you enter an impermissible value (e.g., an impermissible number in an IP address) and then click on the **Apply** button, the relevant tab page title is displayed in red. This makes it easier to trace the error.

Working with sortable tables

Many settings are saved as data records. Accordingly, the adjustable parameters and their values are presented in the form of table rows. If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. Therefore, note the order of the entries, if necessary. The order can be changed by moving table rows up or down.

With tables you can:

– Insert rows to create a new data record with settings (e.g., the firewall settings for a specific connection)

– Move rows (i.e., resort them)

– Delete rows to delete the entire data record

Inserting rows
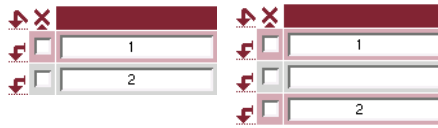
1. Click on the ⬅ arrow below which you want to insert a new row.
2. The new row is inserted.

   You can now enter or specify values in the row.

Moving rows
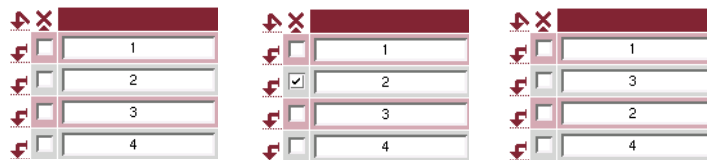
1. Select the row(s) you want to move.
2. Click on the ⬅ arrow below which you want to move the selected rows.
3. The rows are moved.

Deleting rows
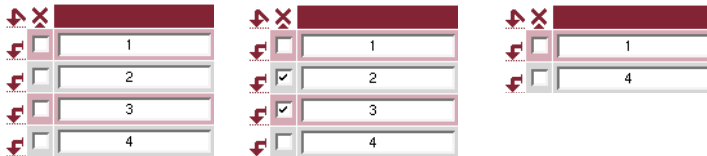
1. Select the rows you want to delete.
2. Click on ✖ to delete the rows.
3. The rows are deleted.

Working with non-sortable tables

Tables are non-sortable if the order of the data records contained within them does not play any technical role. It is then not possible to insert or move rows. With these tables you can:

– Delete rows
– Append rows to the end of the table in order to create a new data record with settings (e.g., user firewall templates)

The symbols for inserting a new table row are therefore different:

– ⬇ to append rows to a **non**-sortable table

– ⬅ to insert rows in a sortable table

Appending rows (non-sortable tables)

1. Click on the ⬇ arrow to append a new row.
2. The new row is appended below the existing table.
   You can now enter or specify values in the row.

Buttons

The following buttons are located at the top of every page:

Logout	For logging out after configuration access to the FL MGUARD.
	If the user does not log out, he/she is logged out automatically if there has been no further activity and the time period specified by the configuration has elapsed. Access can only be restored by logging in again.
Reset	Optional button.
	Resets to the original values. If you have entered values on a configuration page and these have not yet taken effect (by clicking on the **Apply** button), you can restore the original values on the page by clicking the **Reset** button.
	This button only appears at the top of the page if the scope of validity of the **Apply** button is set to "*Include all pages*" (see "Management >> Web Settings" on page 68).
Apply	Optional button.
	Has the same function as the **Apply** button, but is valid for all pages.
	This button only appears at the top of the page if the scope of validity of the **Apply** button is set to "*Include all pages*" (see "Management >> Web Settings" on page 68).

5.2   Management menu

i For security reasons, we recommend you change the default root and administrator passwords during initial configuration (see "Authentication >> Administrative Users" on page 156). A message informing you of this will continue to be displayed at the top of the page until the passwords are changed.

5.2.1   Management >> System Settings

5.2.1.1   Host

Management >> System Settings >> Host	
System	
	Uptime — Device operating time since the last restart.
	(FL MGUARD RS4000/RS2000 only)
	Power supply 1/2 — State of both power supply units (does not apply to FL MGUARD RS2000)
	(FL MGUARD RS4000/RS2000, FL MGUARD SMART2 only)
	System Temperature (°C) — An SNMP trap is triggered if the temperature exceeds or falls below the specified temperature range.

Management >> System Settings >> Host [...]		
System DNS Hostname	**Hostname mode**	You can assign a name to the FL MGUARD using the *Hostname mode* and *Hostname* fields. This name is then displayed, for example, when logging in via SSH (see "Management >> System Settings" on page 50, "Shell Access" on page 58). Assigning names simplifies the administration of multiple FL MGUARD devices.
		User defined (from field below)
		(Default) The name entered in the "Hostname" field is the name used for the FL MGUARD.
		If the FL MGUARD is running in *Stealth* mode, the "User defined" option must be selected under "Hostname mode".
		Provider defined (e.g., via DHCP)
		If the selected network mode permits external setting of the host name, e.g., via DHCP, the name supplied by the provider is assigned to the FL MGUARD.
	Hostname	If the "User defined" option is selected under "Hostname mode", enter the name that should be assigned to the FL MGUARD here.
		Otherwise, this entry will be ignored (i.e., if the "Provider defined" option (e.g., via DHCP) is selected under "Hostname mode").
	Domain search path	This option makes it easier for the user to enter a domain name. If the user enters the domain name in an abbreviated form, the FL MGUARD completes the entry by appending the domain suffix that is defined here under "Domain search path".
SNMP Information	**System Name**	A name that can be freely assigned to the FL MGUARD for administration purposes, e.g., "Hermes", "Pluto". (Under SNMP: sysName)
	Location	A description of the installation location that can be freely assigned, e.g., "Hall IV, Corridor 3", "Control cabinet". (Under SNMP: sysLocation)
	Contact	The name of the contact person responsible for the FL MGUARD, ideally including the phone number. (Under SNMP: sysContact)

5.2.1.2 Signal Contact

The signal contact is a relay that is used by the FL MGUARD to signal error states (see also "Signal contact (alarm output)" on page 22)

Management >> System Settings >> Signal Contact		
Mode	(FL MGUARD RS4000/RS2000 only)	
	Signal contact	The signal contact can be controlled automatically using **Operation supervision** (default) or **Manual settings**.
		See also: "Installing the FL MGUARD RS4000/RS2000" on page 20
Operation supervision	**Contact**	Displays the state of the signal contact Either **Open (Error)** or **Closed (OK)**.
	Redundant power supply	If set to **Ignore**, the power supply does not influence the signal contact.
		If set to **Supervise**, the signal contact is opened if one of the two supply voltages fails.
	Link supervision	Monitoring of the link status of the Ethernet connections. Possible settings are: – Ignore – Supervise internal only (trusted) – Supervise external only (untrusted) – Supervise both
	Temperature state	The signal contact indicates overtemperature and undertemperature. The permissible range is set under *"System Temperature (°C)"* in the *Management >> System Settings >> Host* menu.
		If set to **Ignore**, the temperature does not influence the signal contact.
		If set to **Supervise**, the signal contact is opened if the temperature is not within the permissible range.

Management >> System Settings >> Signal Contact [...]

	Redundancy connection status	Only if the "Redundancy" function is used (see Section 6).
		If set to **Ignore**, the connectivity check does not influence the signal contact.
		If set to **Supervise**, the signal contact is opened if the connectivity check fails. This depends on the state of the FL MGUARD, whether it is active or in standby mode.
Manual settings	**Contact**	If **Signal contact** has been set to **Manual settings**, the contact can be set to **Closed** or **Open (Alarm)** here.

5.2.1.3   Time and Date

Set the time and date correctly. Otherwise, certain time-dependent activities cannot be started by the FL MGUARD (see "Time-controlled activities" on page 54).

Management >> System Settings >> Time and Date

Time and Date	**Current system time (UTC)**	The current system time is displayed as Universal Time Coordinates (UTCs). If **NTP time synchronization** is not yet activated (see below) and **Time-stamp in filesystem** is deactivated, the clock will start at January 1, 2000.
	Current system time (local)	Display: If the (sometimes different) current local time should be displayed, the corresponding entry must be made under **Timezone in POSIX.1 notation...** (see below).
	System time state	Display: Indicates whether the FL MGUARD system time has ever been synchronized with a currently valid time during FL MGUARD runtime. If the display indicates that the FL MGUARD system time has not been synchronized, the FL MGUARD does not perform any time-controlled activities. These are as follows:

Management >> System Settings >> Time and Date [...]	
	Time-controlled activities
	– **Time-controlled pick-up of configuration from a configuration server:**
	This is the case when the *Time Schedule* setting is selected under the *Management >> Central Management* , *Configuration Pull* menu item for the **Pull Schedule** setting (see "Management >> Configuration Profiles" on page 85, "Configuration Pull" on page 100).
	– **Interruption of the connection at a certain time using PPPoE network mode:**
	This is the case when **Network Mode** is set to PPPoE under the *Network >> Interfaces , General* menu item, and **Automatic Reconnect** is set to Yes (see 5.3.1 "Network >> Interfaces", ""Router" network mode, "PPPoE" router mode" on page 126).
	– **Acceptance of certificates when the system time has not yet been synchronized:**
	This is the case when the *Wait for synchronization of the system time* setting is selected under the Authentication >> Certificates , *Certificate settings* menu item for the **Check the validity period of certificates and CRLs** option (see Section 5.4.4 and "Certificate settings" on page 169).
	– **CIFS integrity checking**
	The regular, automatic check of the network drives is only started when the FL MGUARD has a valid time and date (see the following section).
	The system time can be set or synchronized by various events:
	– The FL MGUARD has a built-in clock, which has been synchronized with the current time at least once. The FL MGUARD only has a built-in clock if the **Hardware clock state** field is visible. The display shows whether the clock is synchronized. A synchronized built-in clock ensures that the FL MGUARD has a synchronized system time even after a restart.
	– The administrator has defined the current time for the FL MGUARD runtime by making a corresponding entry in the **Local system time** field.
	– The administrator has set the **Time-stamp in filesystem** setting to *Yes*, and has either transmitted the current system time to the FL MGUARD via NTP (see below under *NTP Server*) or has entered it under **Local system time**. The system time of the FL MGUARD is then synchronized using the time stamp after a restart (even if it has no built-in clock and is set exactly again afterwards via NTP).
	– The administrator has activated NTP time synchronization under **NTP Server**, has entered the address of at least one NTP server, and the FL MGUARD has established a connection with at least one of the specified NTP servers. If the network is working correctly, this occurs a few seconds after a restart. The display in the **NTP State** field may only change to "synchronized" much later (see the explanation below under **NTP State**).

Management >> System Settings >> Time and Date [...]		
	Hardware clock state	(*FL MGUARD RS4000/RS2000* and *FL MGUARD SMART2* only)
		The state of the built-in clock is only visible if the FL MGUARD has a clock that also runs when the FL MGUARD is not supplied with power and is switched off. The display shows whether the clock has been synchronized with the current time. The built-in clock is always synchronized when the system time of the FL MGUARD has been synchronized.
		Once the clock has been synchronized, its state only returns to "not synchronized" if the firmware is reinstalled on the device (see Section 7.3) or
		– if the battery (FL MGUARD RS4000/RS2000, FL MGUARD SMART2)
		did not supply the built-in clock with sufficient voltage for a period when the device was switched off.
	Local system time	Here you can set the FL MGUARD time if no NTP server has been set up (see below) or the NTP server cannot be accessed.
		The date and time are specified in the format YYYY.MM.DD-HH:MM:SS:
		YYYY Year
		MM Month
		DD Day
		HH Hour
	Timezone in POSIX.1 notation...	If a current local time (that differs from Greenwich Mean Time) is to be displayed under *Current system time*, you must enter the number of hours that your local time is ahead of or behind Greenwich Mean Time.
		Example: In Berlin, the time is one hour ahead of GMT. Therefore, enter: CET-1.
		In New York, the time is five hours behind Greenwich Mean Time. Therefore, enter: CET+5.
		The only important thing is the -1, -2 or +1, etc. value as only these values are evaluated – not the preceding letters. They can be "CET" or any other designation, such as "UTC".
		If you wish to display Central European Time (e.g., for Germany) and have it automatically switch to/from daylight saving time, enter: CET-1CEST,M3.5.0,M10.5.0/3

Management >> System Settings >> Time and Date [...]		
	Time-stamp in filesystem (2h granularity): Yes/No	If this option is set to **Yes**, the FL MGUARD writes the current system time to its memory every two hours.
		If the FL MGUARD is switched off and then on again, a time from this two-hour period is displayed, not a time on January 1, 2000.
NTP Server		(NTP - Network Time Protocol) The FL MGUARD can act as the NTP server for computers that are connected to its LAN port. In this case, the computers should be configured so that the local address of the FL MGUARD is specified as the NTP server address.
		If the FL MGUARD is operated in *Stealth* mode, the management IP address of the FL MGUARD (if this is configured) must be used for the computers, or the IP address 1.1.1.1 must be entered as the local address of the FL MGUARD.
		In order for the FL MGUARD to act as the NTP server, it must obtain the current date and the current time from an NTP server (time server). To do this, the address of at least one NTP server must be specified. This feature must also be activated.
	Enable NTP time synchronization: Yes/No	Once the NTP is activated, the FL MGUARD obtains the date and time from one or more time server(s) and synchronizes itself with it or them.
		Initial time synchronization can take up to 15 minutes. During this time, the FL MGUARD continuously compares the time data of the external time server and that of its own time so that this can be adjusted as accurately as possible. Only then the FL MGUARD can act as the NTP server for the computers connected to its LAN interface and provide them with the system time.
		An initial time synchronization with the external time server is performed after every booting process, unless the FL MGUARD has a built-in clock (*FL MGUARD RS4000/RS2000*, *FL MGUARD DELTA TX/TX* and *FL MGUARD SMART2*). After initial time synchronization, the FL MGUARD regularly compares the system time with the time servers. Fine adjustment of the time is usually only made in the second range.
	NTP State	Displays the current NTP status.
		Shows whether the NTP server running on the FL MGUARD has been synchronized with the configured NTP servers to a sufficient degree of accuracy.
		If the system clock of the FL MGUARD has never been synchronized prior to activation of NTP time synchronization, then synchronization can take up to 15 minutes. The NTP server still changes the FL MGUARD system clock to the current time after a few seconds, as soon as it has successfully contacted one of the configured NTP servers. The system time of the FL MGUARD is then regarded as synchronized. Fine adjustment of the time is usually only made in the second range.

Management >> System Settings >> Time and Date [...]		
	NTP Server	Enter one or more time servers from which the FL MGUARD should obtain the current time. If several time servers are specified, the FL MGUARD will automatically connect to all of them to determine the current time.

5.2.1.4   Shell Access

Displayed when
*Enable X.509
certificates for SSH
access* is set to **Yes**

ℹ	The FL MGUARD must not be simultaneously configured via the web access, shell access, or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

Management >> System Settings >> Shell Access	
Shell Access	When SSH remote access is enabled, the FL MGUARD can be configured **from remote computers** using the command line.
	This option is disabled by default.
	ⓘ **NOTE:** If remote access is enabled, ensure that secure passwords are defined for *root* and *admin*.
	Make the following settings for SSH remote access:
	Session Timeout (seconds) — Specifies after what period of inactivity (in seconds) the session is automatically terminated, i.e., automatic logout. When set to 0 (default settings), the session is not terminated automatically.
	The specified value is also valid for shell access via the serial interface instead of via the SSH protocol.
	The effects of the "Session Timeout" field settings are temporarily ineffective if processing of a shell command exceeds the number of seconds set.
	In contrast, the connection can also be aborted if it is no longer able to function correctly, see "Delay between requests for a sign of life" on page 60.
	Enable SSH remote access: Yes/No — If you want to enable SSH remote access, set this option to **Yes**. *Internal* SSH access (i.e., from the directly connected LAN or from the directly connected computer) can be enabled independently of this setting.
	The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access options on the FL MGUARD.
	Port for incoming SSH connections (remote administration only) — Standard: 22
	If this port number is changed, the new port number only applies for access via the *External, External 2, VPN*, and *Dial-in* interface. Port number 22 still applies for internal access.
	The remote partner that implements remote access may have to specify the port number defined here during login.
	Example:
	If this FL MGUARD can be accessed over the Internet via address 123.124.125.21 and default port number 22 has been specified for remote access, you may not need to enter this port number in the SSH client (e.g., PuTTY or OpenSSH) of the remote partner.
	If a different port number has been set (e.g., 2222), this must be specified, e.g.,: ssh -p 2222 123.124.125.21

Management >> System Settings >> Shell Access [...]		
	Delay between requests for a sign of life	Default: 120 seconds
		Values from 0 to 3600 seconds can be set. Positive values indicate that the FL MGUARD is sending a query to the partner within the encrypted SSH connection to find out whether it can still be accessed. The request is sent if no activity was detected from the partner for the specified number of seconds (e.g., due to network traffic within the encrypted connection).
		The value entered relates to the functionality of the encrypted SSH connection. As long as the functions are working properly, the SSH connection is not terminated by the FL MGUARD as a result of this setting, even when the user does not perform any actions during this time.
		Because the number of simultaneously open sessions is limited (see *Concurrent Session Limits*), it is important to terminate sessions that have expired.
		Therefore, the request for a sign of life is preset to 120 seconds in the case of Version 7.4.0 or later. If a maximum of three requests for a sign of life are issued, this causes an expired session to be detected and removed after six minutes.
		In previous versions, the preset was "0". This means that no requests for a sign of life are sent.
		If it is important not to generate additional traffic, you can adjust the value. When the setting "0" is made in conjunction with "*Concurrent Session Limits* ", subsequent access may be blocked if too many sessions are interrupted but not closed as a result of network errors.
	Maximum number of missing signs of life	Specifies the maximum number of times a sign of life request to the partner may remain unanswered.
		For example, if a sign of life request should be made every 15 seconds and this value is set to 3, the SSH connection is deleted if a sign of life is still not detected after approximately 45 seconds.
	Renew SSH and HTTPS key	**Generate new 2048-bit keys**
		Keys that have been generated using a older firmware might be weak and should be renewed.
		• Click on this button to generate a new key.
		• Observe the fingerprints of the new keys generated.
		• Login via HTTPS and compare the certificate information provided by the browser.

Management >> System Settings >> Shell Access [...]

Concurrent Session Limits	In the case of administrative access to the FL MGUARD via SSH, the number of simultaneous sessions is limited, depending on the predefined user. Approximately 0.5 Mbytes of memory space are required for each session.
	The "root" user has unrestricted access. In the case of administrative access via another user *(admin, netadmin,* and *audit),* the number of simultaneous sessions is restricted. You can specify the number here.
	The restriction does not affect existing sessions; it only affects newly established access instances.

Maximum number of concurrent sessions for role "admin"	2 to 2147483647
	At least two simultaneously permitted sessions are required for "admin" to prevent it from having its access blocked.
Maximum number of concurrent sessions for "netadmin" role	0 to 2147483647
	When "0" is set, no session is permitted. The "netadmin" user is not necessarily used.
Maximum number of concurrent sessions for role "audit"	0 to 2147483647
	When "0" is set, no session is permitted. The "audit" user is not necessarily used.

Allowed Networks

	N°	From IP	Interface	Action	Comment	Log
	1	10.1.0.0/16	External ▼	Accept ▼		No ▼
	2	192.168.67.0/24	External ▼	Accept ▼		No ▼

Lists the firewall rules that have been set up. These apply for incoming data packets of an SSH remote access attempt.

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

> **i** The rules specified here only take effect if **Enable SSH remote access** is set to **Yes**. *Internal* access is also possible when this option is set to **No**. A firewall rule that would refuse *Internal* access does therefore not apply in this case.

The following options are available:

From IP	Enter the address of the computer or network from which remote access is permitted or forbidden in this field.
	The following options are available:
	IP address **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format, see "CIDR (Classless Inter-Domain Routing)" on page 294.

Management >> System Settings >> Shell Access [...]			
	Interface	**External/Internal/External 2/VPN/Dial-in**	
		External 2 and *Dial-in* are only for devices with a serial interface, see "Network >> Interfaces" on page 104.	
		Specifies to which interface the rule should apply.	
		If no rules are set or if no rule applies, the following default settings apply:	
		SSH access is permitted via *Internal*, *VPN*, and *Dial-in*. Access via *External* and *External 2* is refused.	
		Specify the access options according to your requirements.	
			NOTE: If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action. **To prevent your own access being blocked**, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Apply** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.
	Action	Options: – **Accept** means that the data packets may pass through. – **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) – **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.	
	Comment	Freely selectable comment for this rule.	
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)	

Management >> System Settings >> Shell Access [...]		
RADIUS Authentication This menu item is not included in the scope of functions for the FL MGUARD RS2000.	**Use RADIUS authentication for Shell access**	If set to **No**, the passwords of users who log in via shell access are checked via the local database on the FL MGUARD. Select **Yes** to enable users to be authenticated via a RADIUS server. This also applies for users who want to access the FL MGUARD via shell access using SSH or a serial console. The password is only checked locally in the case of predefined users *(root, admin, netadmin,* and *audit)*. Under **X.509 Authentication** , if you set **Enable X.509 certificates for SSH access:** to **Yes**, the X.509 authentication procedure can be used as an alternative. Which procedure is actually used by the user depends on how the user uses the SSH client. When setting up a RADIUS authentication for the first time, select **Yes**. ⓘ You should only select **As only method for password authentication** if you are an experienced user, as doing so could result in all access to the FL MGUARD being blocked. If you do intend to use the **As only method for password authentication** option when setting up RADIUS authentication, we recommend that you create a "Customized Default Profile" which resets the authentication method. The predefined users *(root, admin, netadmin,* and *audit)* are then no longer able to log in to the FL MGUARD via SSH or serial console. There is one exception: It it still possible to perform authentication via an externally accessible serial console by correctly entering the local password for the *root* user name.

X.509 authentication

Management >> System Settings >> Shell Access		

X.509 Authentication
 	
This menu item is not included in the scope of functions for the FL MGUARD RS2000.
	Enable X.509 certificates for SSH access:	– If **No** is selected, then only conventional authentication methods (user name and password or private and public keys) are permitted, not the X.509 authentication method.
		– If **Yes** is selected, then the X.509 authentication method can be used in addition to conventional authentication methods (as also used for No).
		– If **Yes** is selected, the following must be specified:
		  – How the FL MGUARD authenticates itself to the SSH client according to X.509, see **SSH server certificate (1)**
		  – How the FL MGUARD authenticates the remote SSH client according to X.509, see **SSH server certificate (2)**

	SSH server certificate (1)	**Specifies how the FL MGUARD identifies itself to the SSH client.** Select one of the machine certificates from the list or the *None* entry. *None*: When *None* is selected, the SSH server of the FL MGUARD does not authenticate itself to the SSH client via the X.509 certificate. Instead, it uses a server key and thus behaves in the same way as older versions of the FL MGUARD. If one of the machine certificates is selected, this is also offered to the SSH client. The client can then decide whether to use the conventional authentication method or the method according to X.509. The selection list contains the machine certificates that have been loaded on the FL MGUARD under the *Authentication >> Certificates* menu item (see Page 163).

Management >> System Settings >> Shell Access [...]

	SSH server certificate (2)	**Specifies how the FL MGUARD authenticates the SSH client.**
		The following definition relates to how the FL MGUARD verifies the authenticity of the SSH client.
		The table below shows which certificates must be provided for the FL MGUARD to authenticate the SSH client if the SSH client shows one of the following certificate types when a connection is established:
		– A certificate signed by a CA
		– A self-signed certificate
		For additional information about the table, see Section 5.4.4, "Authentication >> Certificates".

Authentication for SSH

The partner shows the following:	Certificate (specific to individual), **signed by CA**	Certificate (specific to individual), **self-signed**
The FL MGUARD authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter	Remote certificate

According to this table, the certificates that must be provided are the ones the FL MGUARD uses to authenticate the relevant SSH client.

The following instructions assume that the certificates have already been correctly installed on the FL MGUARD (see Section 5.4.4, "Authentication >> Certificates").

ℹ | If the use of revocation lists (CRL checking) is activated under the *Authentication >> Certificates , Certificate settings* menu item, each certificate signed by a CA that is "shown" by SSH clients is checked for revocations.

Management >> System Settings >> Shell Access

	CA certificate	This configuration is only necessary if the SSH client shows a certificate signed by a CA.
		All CA certificates required by the FL MGUARD to form the chain to the relevant root CA certificate with the certificates shown by the SSH client must be configured.
		The selection list contains the CA certificates that have been loaded on the FL MGUARD under the *Authentication >> Certificates* menu item.

Management >> System Settings >> Shell Access [...]

	X.509 subject	Enables a filter to be set in relation to the contents of the *Subject* field in the certificate shown by the SSH client. It is then possible to limit or enable access for SSH clients, which the FL MGUARD would accept based on certificate checks:

– Limited access to certain *subjects* (i.e., individuals) and/or to *subjects* that have certain attributes
– Access enabled for all subjects

> **i** The *X.509 subject* field must not be left empty.

Access enabled for all subjects (i.e., individuals):

An * (asterisk) in the *X.509 subject* field can be used to specify that all subject entries in the certificate shown by the SSH client are permitted. It is then no longer necessary to identify or define the subject in the certificate.

Limited access to certain subjects (i.e., individuals) or to subjects that have certain attributes:

In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value.

Example: CN=John Smith, O=Smith and Co., C=US

If certain subject attributes have very specific values for the acceptance of the SSH client by the FL MGUARD, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard.

Example: CN=*, O=*, C=US   (with or without spaces between attributes)

In this example, the attribute "C=US" must be entered in the certificate under "Subject". It is only then that the FL MGUARD would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value.

> **i** If a subject filter is set, the number (but not the order) of the specified attributes must correspond to that of the certificates for which the filter is to be used.
>
> Please note that the filter is case-sensitive.

> **i** Several filters can be set and their sequence is irrelevant.

Management >> System Settings >> Shell Access [...]		
	Authorized for access as	All users/root/admin/netadmin/audit
		Additional filter which specifies that the SSH client has to be authorized for a specific administration level in order to gain access.
		When establishing a connection, the SSH client shows its certificate and also specifies the system user for which the SSH session is to be opened (*root, admin, netadmin, audit*). Access is only granted if the entries match those defined here.
		Access for all listed system users is possible when *All users* is set.
		ℹ The *netadmin* and *audit* setting options relate to access rights with the Innominate Device Manager.
	Client certificate	Configuration is required in the following cases: – SSH clients each show a self-signed certificate. – SSH clients each show a certificate signed by a CA. Filtering should take place: Access is only granted to a user whose certificate copy is installed on the FL MGUARD as the remote certificate and is provided to the FL MGUARD in this table as the *Client certificate*. This filter is **not** subordinate to the *Subject* filter. It resides on the same level and is allocated a logical OR function with the *Subject* filter.
		The entry in this field defines which remote certificate the FL MGUARD should adopt in order to authenticate the partner (SSH client).
		The remote certificate can be selected from the selection list. The selection list contains the remote certificates that have been loaded on the FL MGUARD under the *Authentication >> Certificates* menu item.
	Authorized for access as	All users/root/admin/netadmin/audit
		Filter which specifies that the SSH client has to be authorized for a specific administration level in order to gain access.
		When establishing a connection, the SSH client shows its certificate and also specifies the system user for which the SSH session is to be opened (*root, admin, netadmin, audit*). Access is only granted if the entries match those defined here.
		Access for all listed system users is possible when *All users* is set.
		ℹ The *netadmin* and *audit* setting options relate to access rights with the Innominate Device Manager.

5.2.2 Management >> Web Settings

5.2.2.1 General
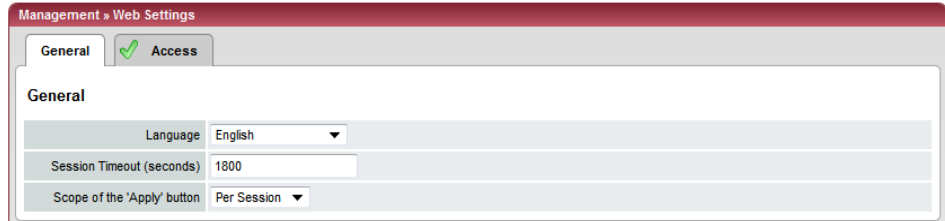
Management >> Web Settings >> General		
General	**Language**	If **(automatic)** is selected in the list of languages, the device uses the language setting of the computer's browser.
	Session Timeout (seconds)	Specifies the period of inactivity (in seconds) after which the user will be automatically logged out of the FL MGUARD web interface. Possible values: 15 to 86400 (= 24 hours)
	Scope of the "Apply" button	The **Per Page** setting specifies that you have to click on the **Apply** button on every page where you make changes in order for the settings to be applied and take effect on the FL MGUARD. The **Per Session** setting specifies that you only have to click on **Apply** once after making changes on a number of pages.

5.2.2.2 Access

Only displayed when *Login with X.509 user certificate* is selected

---

ℹ The FL MGUARD must not be simultaneously configured via the web access, shell access, or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

When web access via HTTPS protocol is enabled, the FL MGUARD can be configured **from a remote computer** using its web-based administrator interface. This means that a browser on the remote computer is used to configure the FL MGUARD.

This option is disabled by default.

⊘ **NOTE:** If remote access is enabled, ensure that secure passwords are defined for *root* and *admin*.

To enable HTTPS remote access, make the following settings:

Management >> Web Settings >> Access		
HTTPS Web Access	**Enable HTTPS remote access: Yes/No**	If you want to enable HTTPS remote access, set this option to **Yes**. *Internal* HTTPS access (i.e., from the directly connected LAN or from the directly connected computer) can be enabled independently of this setting.
		The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access options on the FL MGUARD.
		In addition, the authentication rules under **User authentication** must be set, if necessary.
	Remote HTTPS TCP Port	Standard: 443
		If this port number is changed, the new port number only applies for access via the *External, External 2, VPN*, and *Dial-in* interface. Port number 443 still applies for internal access.
		The remote partner that implements remote access may have to specify the port number defined here after the IP address during entry of the address.
		Example:
		If this FL MGUARD can be accessed over the Internet via address 123.124.125.21 and port number 443 has been specified for remote access, you do not need to enter this port number after the address in the web browser of the remote partner.
		If a different port number is used, it should be entered after the IP address, e.g.,: https://123.124.125.21:442/
		ⓘ The FL MGUARD authenticates itself to the partner, in this case the browser of the user, using a self-signed machine certificate. This is a unique certificate issued by Innominate for each FL MGUARD. This means that every FL MGUARD device is delivered with a unique, self-signed machine certificate.
	Renew SSH and HTTPS key	**Generate new 2048-bit keys**
		Keys that have been generated using a older firmware might be weak and should be renewed.
		• Click on this button to generate a new key.
		• Observe the fingerprints of the new keys generated.
		• Login via HTTPS and compare the certificate information provided by the browser.
Allowed Networks		

N°	From IP	Interface	Action	Comment	Log
1	0.0.0.0/0	External ▼	Accept ▼		No ▼

Management >> Web Settings >> Access [...]

Lists the firewall rules that have been set up. These apply for incoming data packets of an HTTPS remote access attempt.

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

The rules specified here only take effect if **Enable HTTPS remote access** is set to **Yes**. *Internal* access is also possible when this option is set to **No**. A firewall rule that would refuse *Internal* access does therefore not apply in this case.

The following options are available:

From IP
Enter the address of the computer or network from which remote access is permitted or forbidden in this field.

IP address **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format – see "CIDR (Classless Inter-Domain Routing)" on page 294.

Interface
External/Internal/External 2/VPN/Dial-in[1]

Specifies to which interface the rule should apply.

If no rules are set or if no rule applies, the following default settings apply:

HTTPS access is permitted via *Internal, VPN*, and *Dial-in*. Access via *External* and *External 2* is refused.

Specify the access options according to your requirements.

> **i** If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action. **To prevent your own access being blocked**, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Apply** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.

Action
– **Accept** means that the data packets may pass through.
– **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.)
– **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.

Comment
Freely selectable comment for this rule.

Management >> Web Settings >> Access [...]

	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)
RADIUS Authentication This menu item is not included in the scope of functions for the FL MGUARD RS2000.	**Enable RADIUS authentication**	If set to **No**, the passwords of users who log in via HTTPS are checked via the local database. The **User authentication method** can only be set to **Login restricted to X.509 client certificate** if **No** is selected. Select **Yes** to enable users to be authenticated via the RADIUS server. The password is only checked locally in the case of predefined users (*root*, *admin*, *netadmin*, *audit,* and *user)*. ⚫ⓘ You should only select **As only method for password authentication** if you are an experienced user, as doing so could result in all access to the FL MGUARD being blocked. When setting up a RADIUS authentication for the first time, select **Yes**. If you do intend to use the **As only method for password authentication** option when setting up RADIUS authentication, we recommend that you create a "Customized Default Profile" which resets the authentication method. If you have selected RADIUS authentication as the only method for checking the password, it may no longer be possible to access the FL MGUARD. For example, this may be the case if you set up the wrong RADIUS server or convert the FL MGUARD. The predefined users (*root*, *admin*, *netadmin*, *audit,* and *user)* are then no longer accepted.

¹ *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 104).

Management >> Web Settings >> Access

User authentication

This menu item is not included in the scope of functions for the FL MGUARD RS2000.

User authentication

| User authentication method | Login with X.509 client certificate or password ▼ |

| CA certificate |
| VPN-RootCA 01 ▼ |

| X.509 Subject | Authorized for access as |
| | root ▼ |

| X.509 Certificate | Authorized for access as |
| Battaglia\, Mauro ▼ | root ▼ |

Defines how the local FL MGUARD authenticates the remote partner	**User authentication method**

Login with password

Specifies that the remote FL MGUARD user must use a password to log into the FL MGUARD. The password is specified under the *Authentication >> Administrative Users* menu (see Page 156). The option of RADIUS authentication is also available (see Page 161).

Depending on which user ID is used to log in (user or administrator password), the user has the right to operate and/or configure the FL MGUARD accordingly.

Login with X.509 client certificate or password

– User authentication is by means of login with a password (see above).
– The user's browser authenticates itself using an X.509 certificate and a corresponding private key. Additional details must be specified below.

The use of either method depends on the web browser of the remote user. The second option is used when the web browser provides the FL MGUARD with a certificate.

Login restricted to X.509 client certificate

The user's browser must use an X.509 certificate and the corresponding private key to authenticate itself. Additional details must be specified here.

> **i** Before enabling the *Login restricted to X.509 client certificate* option, you must first select and test the *Login with X.509 client certificate or password* option.
>
> Only switch to *Login restricted to X.509 client certificate* when you are sure that this setting works. **Otherwise your access could be blocked.**
>
> Always take this precautionary measure when modifying settings under **User authentication**.

If the following **User authentication methods** are defined:
– Login restricted to X.509 client certificate
– Login with X.509 client certificate or password

You must then specify how the FL MGUARD authenticates the remote user according to X.509.

The table below shows which certificates must be provided for the FL MGUARD to authenticate the user (access via HTTPS) if the user or their browser shows one of the following certificate types when a connection is established:
– A certificate signed by a CA
– A self-signed certificate

For additional information about the table, see "Authentication >> Certificates" on page 163.

X.509 authentication for HTTPS

The partner shows the following:	Certificate (specific to individual) **signed by CA**[1]	Certificate (specific to individual), **self-signed**
The FL MGUARD authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter	Remote certificate

[1] The partner can additionally provide sub-CA certificates. In this case, the FL MGUARD can form the set union for creating the chain from the CA certificates provided and the self-configured CA certificates. The corresponding root certificate must always be available on the FL MGUARD.

According to this table, the certificates that must be provided are the ones the FL MGUARD uses to authenticate a remote user (access via HTTPS) or their browser.

The following instructions assume that the certificates have already been correctly installed on the FL MGUARD (see "Authentication >> Certificates" on page 163).

$\mathbf{i}$	If the use of revocation lists (CRL checking) is activated under the Authentication >> Certificates *, Certificate settings* menu item, each certificate signed by a CA that is "shown" by the HTTPS clients must be checked for revocations.

Management >> Web Settings >> Access		
	CA certificate	This configuration is only necessary if the user (access via HTTPS) shows a certificate signed by a CA.
		All CA certificates required by the FL MGUARD to form the chain to the relevant root CA certificate with the certificates shown by the user must be configured.
		If the browser of the remote user also provides CA certificates that contribute to forming the chain, then it is not necessary for these CA certificates to be installed on the FL MGUARD and referenced at this point.
		However, the corresponding root CA certificate must be installed on the FL MGUARD and made available (referenced) in any case.
		$\mathbf{i}$ When selecting the CA certificates to be used or when changing the selection or the filter settings, you must first select and test the *Login with X.509 client certificate or password* option as the *User authentication method* before enabling the (new) setting.
		Only switch to *Login restricted to X.509 client certificate* when you are sure that this setting works. **Otherwise your access could be blocked.**
		Always take this precautionary measure when modifying settings under **User authentication**.

Management >> Web Settings >> Access [...]		
	X.509 Subject	Enables a filter to be set in relation to the contents of the *Subject* field in the certificate shown by the browser/HTTPS client.
		It is then possible to limit or enable access for the browser/HTTPS client, which the FL MGUARD would accept based on certificate checks:
		– Limited access to certain *subjects* (i.e., individuals) and/or to *subjects* that have certain attributes
		– Access enabled for all subjects:
		<table><tr><td>**i**</td><td>The *X.509 subject* field must not be left empty.</td></tr></table>
		Access enabled for all subjects (i.e., individuals):
		An * (asterisk) in the *X.509 subject* field can be used to specify that all subject entries in the certificate shown by the browser/HTTPS client are permitted. It is then no longer necessary to identify or define the subject in the certificate.

Management >> Web Settings >> Access [...]

Limited access to certain subjects (i.e., individuals) and/or to subjects that have certain attributes:

In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value.

Example: CN=John Smith, O=Smith and Co., C=US

If certain subject attributes have very specific values for the acceptance of the browser by the FL MGUARD, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the ***** (asterisk) wildcard.

Example: CN=*, O=*, C=US   (with or without spaces between attributes)

In this example, the attribute "C=US" must be entered in the certificate under "Subject". It is only then that the FL MGUARD would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value.

> **i** If a subject filter is set, the number (but not the order) of the specified attributes must correspond to that of the certificates for which the filter is to be used.
>
> Please note that the filter is case-sensitive.

> **i** Several filters can be set and their sequence is irrelevant.

With HTTPS, the browser of the accessing user does not specify which user or administration rights it is using to log in. These access rights are assigned by setting filters here (under "Authorized for access as").

This has the following result: If there are several filters that "let through" a certain user, then the first filter applies. The user is assigned the access rights as defined by this filter. This could differ from the access rights assigned to the user in the subsequent filters.

> **i** If remote certificates are configured as filters in the **X.509 Certificate** table column, then these filters have priority over the filter settings here.

Management >> Web Settings >> Access [...]		
	Authorized for access as	**All users/root/admin/netadmin/audit**
		Specifies which user or administrator rights are granted to the remote user.
		For a description of the *root, admin*, and *user* authorization levels, see "Authentication >> Administrative Users" on page 156.
		The *netadmin* and *audit* authorization levels relate to access rights with the Innominate Device Manager.
	X.509 Certificate	Configuration is required in the following cases:
		– Remote users each show a self-signed certificate.
		– Remote users each show a certificate signed by a CA. Filtering should take place: Access is only granted to a user whose certificate copy is installed on the FL MGUARD as the remote certificate and is provided to the FL MGUARD in this table as the *X.509 Certificate*.
		If used, this filter has priority over the *Subject* filter in the table above.
		The entry in this field defines which remote certificate the FL MGUARD should adopt in order to authenticate the partner (browser of the remote user).
		The remote certificate can be selected from the selection list.
		The selection list contains the remote certificates that have been loaded on the FL MGUARD under the Authentication >> Certificates menu item.
	Authorized for access as	**root/admin/netadmin/audit/user**
		Specifies which user or administrator rights are granted to the remote user.
		For a description of the *root, admin*, and *user* authorization levels, see "Authentication >> Administrative Users" on page 156.
		The *netadmin* and *audit* authorization levels relate to access rights with the Innominate Device Manager.

5.2.3 Management >> Licensing

5.2.3.1 Overview

With FL MGUARD Version 5.0 or later, licenses remain installed even after the firmware is flashed.

However, licenses are still deleted when devices with older firmware versions are flashed to Version 5.0.0 or later. Before flashing, the license for using the new update must then first be obtained so that the required license file is available for the flashing process.

This applies to major release upgrades, e.g., from Version 4.x.y to Version 5.x.y to Version 6.x.y, etc. (see "Flashing the firmware/rescue procedure" on page 325).

Management >> Licensing >> Overview		
Basic settings	Feature License	Shows which functions are included with the installed FL MGUARD licenses, e.g., the number of possible VPN tunnels, whether remote logging is supported, etc.

5.2.3.2 Install

> **i** This function is **not** available on the **FL MGUARD RS2000**.

More functions can be added later to the FL MGUARD license you have obtained. You will

find a voucher serial number and a voucher key in the voucher included with the FL MGUARD. The voucher can also be purchased separately.

It can be used to:

– Request the required feature license file

– Install the license file that you receive following this request

Management >> Licensing >> Install		
Automatic License Installation	**Voucher Serial Number/Voucher Key**	Enter the serial number printed on the voucher and the corresponding voucher key, then click on **Online License Request**.
		The FL MGUARD now establishes a connection via the Internet and installs the corresponding license on the FL MGUARD if the voucher is valid.
	Reload Licenses	This option can be used if the license installed on the FL MGUARD has been deleted. Click on **Online License Reload**.
		The licenses that were previously issued for this FL MGUARD are then retrieved from the server via the Internet and installed.
Manual License Installation	**Order License** **Filename**	After clicking on **Edit License Request Form**, an online form is displayed, which can be used to order the desired license. Enter the following information in the form: – Voucher Serial Number: The serial number printed on your voucher – Voucher Key: The voucher key on your voucher – Flash ID: This is entered automatically After sending the form, the license file is made available for download and can be installed on the FL MGUARD in a further step. **Install license file** To install a license, first save the license file as a separate file on your computer, then proceed as follows: • Click on **Browse...** next to the *Filename* field. Select the file and open it so that the file name or path is displayed in the *Filename* field. • Then click on **Install license file**.

5.2.3.3   Terms of License

Lists the licenses of the external software used on the FL MGUARD. The software is usually open-source software.

5.2.4 Management >> Update

5.2.4.1 Overview
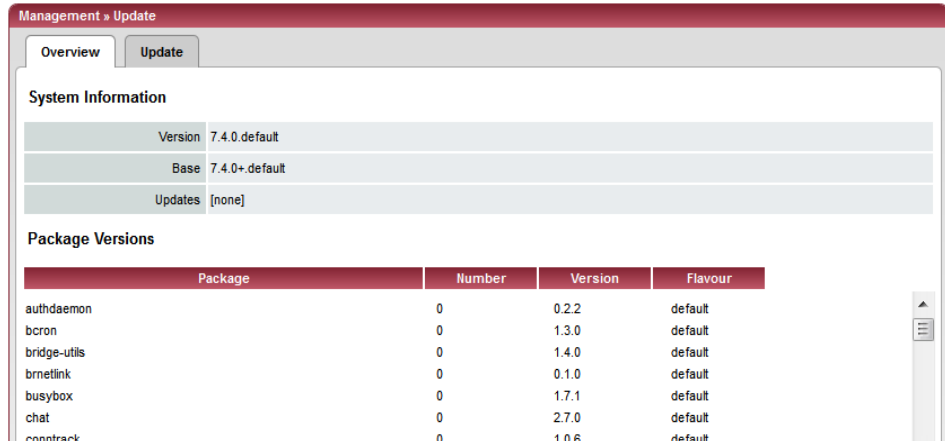
Management >> Update >> Overview		
System Information	**Version**	The current software version of the FL MGUARD.
	Base	The software version that was originally used to flash this FL MGUARD.
	Updates	List of updates that have been installed on the base.
Package Versions	Lists the individual software modules of the FL MGUARD. Can be used for support purposes.	

5.2.4.2 Update

Firmware updates with firewall redundancy enabled

Updates of Version 7.3.1 or later can be performed while an FL MGUARD redundant pair is connected and operating.

This does not apply to the following devices:
– FL MGUARD PCI4000
– FL MGUARD DELTA TX/TX

These devices must be updated successively while the relevant redundant device is disconnected.

If firewall redundancy is activated, the two FL MGUARD devices of a redundant pair can be updated at the same time. FL MGUARD devices that form a pair automatically decide which FL MGUARD is to perform the update first while the other FL MGUARD remains active. If the active FL MGUARD is unable to boot within 25 minutes of receiving the update command (because the other FL MGUARD has not yet taken over), it aborts the update and continues to run using the existing firmware version.

Running a firmware update

There are two options for performing a firmware update:
1. You have the current package set file on your computer (the file name ends with ".tar.gz") and you perform a local update.
2. The FL MGUARD downloads a firmware update of your choice from the update server via the Internet and installs it.
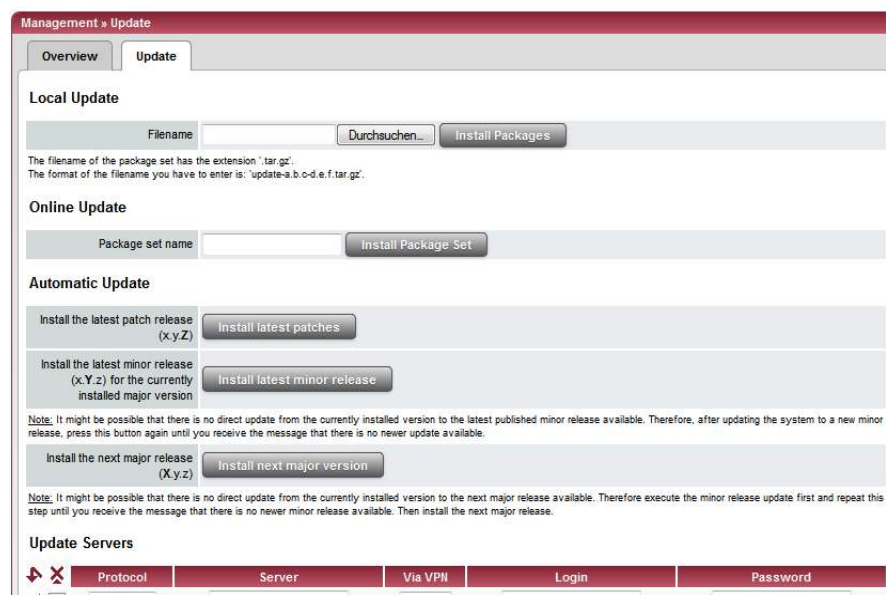
NOTE: Do not interrupt the power supply to the FL MGUARD during the update process. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

Depending on the size of the update, the process may take several minutes.

	A message is displayed if a restart is required after completion of the update.

Management >> Update		
Local Update	**Filename**	To install the packages, proceed as follows: • Click on **Browse...**, select the file, and open it so that the file name or path is displayed in the *Filename* field. The file name must have the following format: update-a.b.c-d.e.f.default.<platform>.tar.gz **Example**: update-7.0.0-7.0.1.default.ixp4xx_be.tar.gz • Then click on **Install Packages**.
Online Update		To perform an online update, proceed as follows: • Make sure that there is at least one valid entry under **Update Servers**. You should have received the necessary details from your licenser. • Enter the name of the package set, e.g., "update-6.1.x-7.2.0". • Then click on **Install Package Set**.
Automatic Update		This is a version of the online update where the FL MGUARD independently determines the required package set.
	Install the latest patch release (x.y.Z)	Patch releases resolve errors in previous versions and have a version number which only changes in the third digit position. For example, 4.0.1 is a patch release for Version 4.0.0.
	Install the latest minor release (x.Y.z) for the currently installed major version	Minor and major releases supplement the FL MGUARD with new properties or contain changes that affect the behavior of the FL MGUARD. Their version number changes in the first or second digit position.
	Install the next major release (X.y.z)	For example, 4.1.0 is a major or minor release for versions 3.1.0 or 4.0.1 respectively.
Update Servers		Specify from which servers an update may be performed.
		The list of servers is processed from top to bottom until an available server is found. The order of the entries therefore also specifies their priority.
		All configured update servers must provide the same updates.
		The following options are available:
	Protocol	The update can be performed via HTTPS or HTTP.
	Server	Host name of the server that provides the update files.

Management >> Update [...]

	Via VPN	The update is performed via the VPN tunnel.
		Default: No.

> ℹ️ Updates via VPN are not supported if the relevant VPN tunnel has been disabled in the configuration (see Section 5.7.2, *IPsec VPN >> Connections*) and has only been temporarily opened via the service contact or CGI interface.

	Login	Login for the server.
	Password	Password for login.

5.2.5   Management >> Configuration Profiles

5.2.5.1   Configuration Profiles
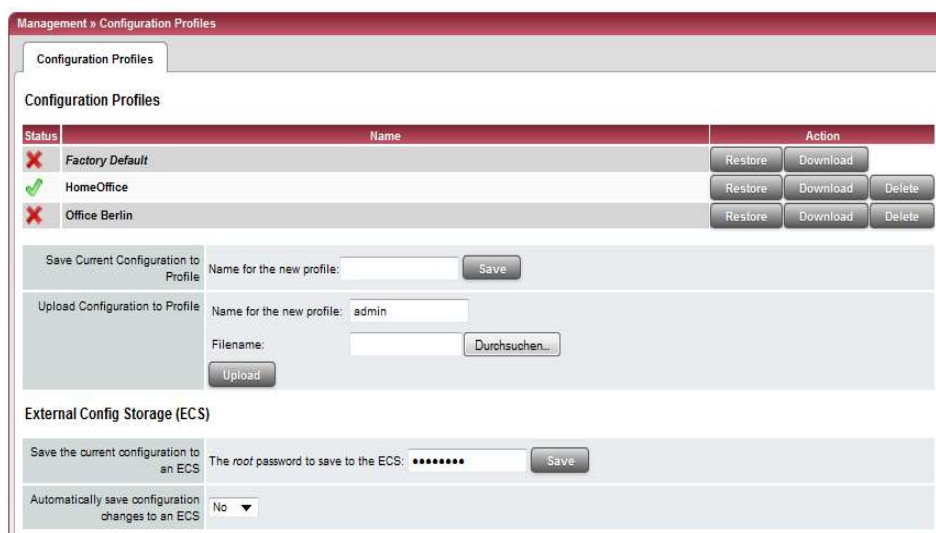
You can save the settings of the FL MGUARD as a configuration profile under any name on the FL MGUARD. It is possible to create multiple configuration profiles. You can then switch between different profiles as required, for example, if the FL MGUARD is used in different environments.

Furthermore, you can also save the configuration profiles as files on your configuration computer. Alternatively, these configuration files can be loaded onto the FL MGUARD and activated.

In addition, you can restore the *Factory Default* settings at any time.

With the FL MGUARD RS4000/RS2000, FL MGUARD DELTA TX/TX, FL MGUARD PCI4000, configuration profiles can also be stored on an external configuration memory, e.g., SD card (FL MGUARD RS4000/RS2000, FL MGUARD DELTA TX/TX, FL MGUARD PCI4000) (see "Profile on external storage medium: FL MGUARD

RS4000/2000, FL MGUARD DELTA TX/TX, FL MGUARD PCI4000" on page 87).

i	When a configuration profile is saved, the passwords used for authenticating administrative access to the FL MGUARD are not saved.

i	It is possible to load and activate a configuration profile that was created under an older firmware version. However, the reverse is not true – a configuration profile created under a newer firmware version should not be loaded.

Management >> Configuration Profiles	
Configuration Profiles	At the top of the page there is a list of the configuration profiles that are stored on the FL MGUARD, e.g., the *Factory Default* configuration profile. If any configuration profiles have been saved by the user (see below), they will be listed here.
	Active configuration profile: The configuration profile that is currently enabled has an *Active* symbol at the start of the entry.
	Configuration profiles that are stored on the FL MGUARD can be:
	– Enabled
	– Saved as a file on the connected configuration computer
	– Deleted
	– Displayed
	Displaying the configuration profile:
	• Click on the name of the configuration profile in the list.
	Enabling the default setting or a configuration profile saved on the FL MGUARD by the user:
	• Click on **Restore** to the right of the name of the relevant configuration profile. The corresponding configuration profile is activated.
	Saving the configuration profile as a file on the configuration computer:
	• Click on **Download** to the right of the name of the relevant configuration profile.
	• In the dialog box that is displayed, specify the file name and folder under which the configuration profile is to be saved as a file. (The file name can be freely selected.)
	Deleting a configuration profile:
	• Click on **Delete** to the right of the name of the relevant configuration profile.
	<table><tr><td>**i**</td><td>The *Factory Default* profile cannot be deleted.</td></tr></table>
Save Current Configuration to Profile	**Saving the active configuration as a configuration profile on the FL MGUARD:**
	• Enter the desired profile name in the *Name for the new profile* field next to "Save Current Configuration to Profile".
	• Click on **Save**. The configuration profile is saved on the FL MGUARD, and the name of the profile appears in the list of profiles already stored on the FL MGUARD.

Management >> Configuration Profiles [...]		
Upload Configuration to Profile	**Uploading a configuration profile that has been saved to a file on the configuration computer:**	
	Requirement: A configuration profile has been saved on the configuration computer as a file according to the procedure described above.	
	• Enter the desired profile name in the *Name for the new profile* field next to "Upload Configuration to Profile".	
	• Click on **Browse...**, select and open the relevant file in the dialog box that is displayed.	
	• Click on **Upload**.	
	The configuration profile is loaded on the FL MGUARD, and the name assigned in step 1 appears in the list of profiles already stored on the FL MGUARD.	
External Config Storage (ECS)	**Save the active configuration to an external memory**	*FL MGUARD RS4000/RS2000,* FL MGUARD DELTA TX/TX, FL MGUARD PCI4000 only
		When replacing the original device with a replacement device, the configuration profile can be applied using the external memory. To do so, the replacement device must still use "root" as the password for the "root" user.
		If the root password on the replacement device is not "root", this password must be entered in the **The root password to save to the ECS** field.
		(See "Saving a profile to an external storage medium")
	Automatically save configuration changes to an external memory	*FL MGUARD RS4000/RS2000,* FL MGUARD DELTA TX/TX, FL MGUARD PCI4000 only
		When set to **Yes**, the configuration changes are automatically saved to the external memory, i.e., the external memory always stores the profile currently used.
		The FL MGUARD only uses the automatically stored configuration profiles upon startup if the original password ("root") is still set on the FL MGUARD for the "root" user (see "Loading a profile from an external storage medium" on page 88).
		Configuration changes are also made, if the external memory is disconnected, full, or defective. The corresponding error messages are displayed in the Logging menu (see Section 5.11.2).
		Activation of the new settings extends the response time of the user interface when changing any settings.

Profile on external storage medium: FL MGUARD RS4000/2000, FL MGUARD DELTA TX/TX, FL MGUARD PCI4000

FL MGUARD RS4000/RS2000, FL MGUARD DELTA TX/TX, FL MGUARD PCI4000:
Configuration profiles can also be stored on an SD card (up to 2 Gbytes capacity). It must have the following characteristics:

– VFAT file system on the first primary partition, at least 64 Mbytes free memory capacity. We recommend using cards from Phoenix Contact. Using cards from other manufacturers is at the user's own risk and Phoenix Contact support is not provided.

Saving a profile to an external storage medium

- **FL MGUARD RS4000/RS2000, FL MGUARD DELTA TX/TX, FL MGUARD PCI4000**: Insert the SD card into the SD slot at the front.
- If the root password on the FL MGUARD onto which the profile is going to be subsequently loaded is not "root", this password must be entered in the **The root password to save to the ECS** field.
- Click on **Save**.

Loading a profile from an external storage medium

- **FL MGUARD RS4000/RS2000, FL MGUARD DELTA TX/TX, FL MGUARD PCI4000**: Insert the SD card into the SD slot at the front.
- Once the storage medium has been inserted, start the FL MGUARD.
- The FL MGUARD root password must either be "root" or correspond to the password that was specified while the profile was being saved.

The configuration profile loaded from the storage medium is loaded onto the FL MGUARD and applied.

The loaded configuration profile does not appear in the list of configuration profiles stored on the FL MGUARD.

The configuration on the external storage medium also contains the passwords for the *root*, *admin*, *netadmin*, *audit*, and *user* users. These passwords are also loaded when loading from an external storage medium.

5.2.6 Management >> SNMP

> ℹ The FL MGUARD must not be simultaneously configured via the web access, shell access, or SNMP. Simultaneous configuration via the different access methods might lead to unexpected results.

5.2.6.1 Query

The SNMP (Simple Network Management Protocol) is mainly used in more complex networks to monitor the state and operation of devices.

SNMP is available in several releases: SNMPv1/SNMPv2 and SNMPv3.

The older versions (SNMPv1/SNMPv2) do not use encryption and are not considered to be secure. The use of SNMPv1/SNMPv2 is therefore not recommended.

SNMPv3 is significantly better in terms of security, but not all management consoles support this version yet.

If SNMPv3 or SNMPv1/v2 is activated, this is indicated by a green signal field on the tab at the top of the page. Otherwise, i.e., if SNMPv3 or SNMPv1/v2 is not active, the signal field is red.

> ℹ Processing an SNMP request may take more than one second. However, this value corresponds to the default timeout value of some SNMP management applications.
> • If you experience timeout problems, set the timeout value of your management application to values between 3 and 5 seconds.

Management >> SNMP >> Query		
Settings	Enable SNMPv3 access: Yes/No	If you wish to allow monitoring of the FL MGUARD via SNMPv3, set this option to **Yes**.
		The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access and monitoring options on the FL MGUARD.
		Access via SNMPv3 requires authentication with a login and password. The default settings for the login parameters are:
		Login: admin
		Password: SnmpAdmin (please note that the password is case-sensitive)
		MD5 is supported for the authentication process; DES is supported for encryption.
		The login parameters for SNMPv3 can only be changed using SNMPv3.
	Enable SNMPv1/v2 access: Yes/No	If you wish to allow monitoring of the FL MGUARD via SNMPv1/v2, set this option to **Yes**.
		You must also enter the login data under **SNMPv1/v2 Community**.
		The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access and monitoring options on the FL MGUARD.
	Port for incoming SNMP connections	Standard: 161
		If this port number is changed, the new port number only applies for access via the *External, External 2, VPN*, and *Dial-in* interface. Port number 161 still applies for internal access.
		The remote partner that implements remote access may have to specify the port number defined here during entry of the address.
SNMPv1/v2 Community	Read-Write Community	Enter the required login data in this field.
	Read-Only Community	Enter the required login data in this field.
Allowed Networks		Lists the firewall rules that have been set up. These apply for incoming data packets of an SNMP access attempt.
		The rules specified here only take effect if **Enable SNMPv3 access** or **Enable SNMPv1/v2 access** is set to **Yes**.
		If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

Management >> SNMP >> Query [...]

	From IP	Enter the address of the computer or network from which remote access is permitted or forbidden in this field. The following options are available: – An IP address – To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294). – **0.0.0.0/0** means all addresses.
	Interface	**External/Internal/External 2/VPN/Dial-in**[1] Specifies to which interface the rule should apply. If no rules are set or if no rule applies, the following default settings apply: SNMP monitoring is permitted via *Internal, VPN*, and *Dial-in*. Access via *External* and *External 2* is refused. Specify the monitoring options according to your requirements. **NOTE:** If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action. **To prevent your own access being blocked**, you may have to permit access simultaneously via another interface explicitly with *Accept* before clicking on the **Apply** button to activate the new setting. Otherwise, if your access is blocked, you must carry out the recovery procedure.
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.) **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)

[1]   *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 104).

5.2.6.2 Trap

In certain cases, the FL MGUARD can send SNMP traps. SNMP traps are only sent if the SNMP request is activated.

The traps correspond to SNMPv1. The trap information for each setting is listed below. A more detailed description can be found in the MIB that belongs to the FL MGUARD.

> **i**   If SNMP traps are sent to the partner via a VPN channel, the IP address of the partner must be located in the network that is specified as the **Remote** network in the definition of the VPN connection.
>
> The internal IP address (in Stealth mode: **Stealth Management IP Address** or **Virtual IP**) must be located in the network that is specified as **Local** in the definition of the VPN connection (see "Defining a VPN connection/VPN connection channels" on page 223).

– If the Enable 1-to-1 NAT of the local network to an internal network option is set to Yes (see "1:1 NAT" on page 236), the following applies:

The internal IP address (in Stealth mode: **Stealth Management IP Address** or **Virtual IP**) must be located in the network that is specified as the **Internal network address for local 1-to-1 NAT**.

– If the Enable 1-to-1 NAT of the remote network to a different network option is set to Yes (see "1:1 NAT" on page 236), the following applies:

The IP address of the trap receiver must be located in the network that is specified as **Remote** in the definition of the VPN connection.

Management >> SNMP >> Trap		
Basic traps	**SNMP authentication**	Activate traps **Yes/No**
		– enterprise-oid : FL MGUARDInfo
		– generic-trap : authenticationFailure
		– specific-trap : 0
		Sent if an unauthorized station attempts to access the FL MGUARD SNMP agent.
	Link Up/Down	Activate traps **Yes/No**
		– enterprise-oid : FL MGUARDInfo
		– generic-trap : linkUp, linkDown
		– specific-trap : 0
		Sent when the connection to a port is interrupted (linkDown) or restored (linkUp).
	Coldstart	Activate traps **Yes/No**
		– enterprise-oid : FL MGUARDInfo
		– generic-trap : coldStart
		– specific-trap : 0
		Sent after a cold restart or warm start.
	Admin access (SSH, HTTPS), new DHCP client	Activate traps **Yes/No**
		– enterprise-oid : FL MGUARD
		– generic-trap : enterpriseSpecific
		– specific-trap : FL MGUARDHTTPSLoginTrap (1)
		– additional : FL MGUARDHTTPSLastAccessIP
		This trap is sent if someone has tried successfully or unsuccessfully (e.g., using an incorrect password) to open an HTTPS session. The trap contains the IP address from which the attempt was issued.
		– enterprise-oid : FL MGUARD
		– generic-trap : enterpriseSpecific
		– specific-trap : FL MGUARDShellLoginTrap (2)
		– additional : FL MGUARDShellLastAccessIP
		This trap is sent when someone opens the shell via SSH or the serial interface. The trap contains the IP address of the login request. If this request was sent via the serial interface, the value is 0.0.0.0.

Management >> SNMP >> Trap [...]		
		– enterprise-oid : FL MGUARD – generic-trap : enterpriseSpecific – specific-trap : 3 – additional : FL MGUARDDHCPLastAccessMAC
		This trap is sent when a DHCP request is received from an unknown client.
		– enterprise-oid : FL MGUARD – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapSSHLogin – additional : FL MGUARDTResSSHUsername 　　　　　　　　 FL MGUARDTResSSHRemoteIP
		This trap is sent when someone accesses the FL MGUARD via SSH.
		– enterprise-oid : FL MGUARD – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapSSHLogout – additional : FL MGUARDTResSSHUsername 　　　　　　　　 FL MGUARDTResSSHRemoteIP
		This trap is sent when access to the FL MGUARD via SSH is terminated.
Hardware related traps (FL MGUARD RS4000/RS2000 only)	**Chassis (power, signal relay)**	Activate traps **Yes/No** – enterprise-oid : FL MGUARDTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapIndustrialPowerStatus (2) – additional : FL MGUARDTrapIndustrialPowerStatus
		Sent when the system registers a power failure.
		– enterprise-oid : FL MGUARDTrapSenderIndustrial – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapSignalRelais (3) – additional : FL MGUARDTResSignalRelaisState 　　　　　　　　 (FL MGUARDTEsSignlalRelaisReason, FL MGUARDTResSignal RelaisReasonIdx)
		Sent after the signal contact is changed and indicates the current status (0 = Off, 1 = On).

Management >> SNMP >> Trap [...]			
	Agent (external config storage, temperature)	Activate traps **Yes/No**	
		– enterprise-oid	: FL MGUARDTrapIndustrial
		– generic-trap	: enterpriseSpecific
		– specific-trap	: FL MGUARDTrapIndustrialTemperature (1)
		– additional	: FL MGUARDSystemTemperature, FL MGUARDTrapIndustrialTempHiLimit, FL MGUARDTrapIndustrialLowLimit
		The trap indicates the temperature in the event of the temperature exceeding the specified limit values.	
		– enterprise-oid	: FL MGUARDTrapIndustrial
		– genericTrap	: enterpriseSpecific
		– specific-trap	: FL MGUARDTrapAutoConfigAdapterState (4)
		– additional	: FL MGUARDTrapAutoConfigAdapter Change
		This trap is sent after access to the external memory.	
CIFS integrity traps This menu item is not included in the scope of functions for the FL MGUARD RS2000.	**Successful integrity check of a CIFS share**	Activate traps **Yes/No**	
		– enterprise-oid	: FL MGUARDTrapCIFSScan
		– generic-trap	: enterpriseSpecific
		– specific-trap	: FL MGUARDTrapCIFSScanInfo (1)
		– additional	: FL MGUARDTResCIFSShare, FL MGUARDTResCIFSScanError, FL MGUARDTResCIFSNumDiffs
		This trap is sent if the CIFS integrity check has been successfully completed.	
	Failed integrity check of a CIFS share	Activate traps **Yes/No**	
		– enterprise-oid	: FL MGUARDTrapCIFSScan
		– generic-trap	: enterpriseSpecific
		– specific-trap	: FL MGUARDTrapCIFSScanFailure (2)
		– additional	: FL MGUARDTResCIFSShare, FL MGUARDTResCIFSScanError, FL MGUARDTResCIFSNumDiffs
		This trap is sent if the CIFS integrity check has failed.	

Management >> SNMP >> Trap [...]		
	Found a (suspicious) difference on a CIFS share	Activate traps **Yes/No** – enterprise-oid : FL MGUARDTrapCIFSScan – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapCIFSScanDetection (3) – additional : FL MGUARDTResCIFSShare, FL MGUARDTResCIFSScanError, FL MGUARDTResCIFSNumDiffs This trap is sent if the CIFS integrity check has detected a deviation.
Userfirewall traps This menu item is not included in the scope of functions for the FL MGUARD RS2000.	**Userfirewall traps**	Activate traps **Yes/No** – enterprise-oid : FL MGUARDTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapUserFirewallLogin (1) – additional : FL MGUARDTResUserFirewallUsername, FL MGUARDTResUserFirewallSrcIP, FL MGUARDTResUserFirewallAuthenticationMethod This trap is sent when a user logs into the user firewall. – enterprise-oid : FL MGUARDTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapUserFirewallLogout (2) – additional : FL MGUARDTResUserFirewallUsername, FL MGUARDTResUserFirewallSrcIP, FL MGUARDTResUserFirewallLogoutReason This trap is sent when a user logs out of the user firewall. – enterprise-oid : FL MGUARDTrapUserFirewall – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapUserFirewallAuthError TRAP-TYPE (3) – additional : FL MGUARDTResUserFirewallUsername, FL MGUARDTResUserFirewallSrcIP, FL MGUARDTResUserFirewallAuthenticationMethod This trap is sent in the event of an authentication error.

Management >> SNMP >> Trap [...]

VPN traps	IPsec connection status changes	Activate traps **Yes/No**
		– enterprise-oid : FL MGUARDTrapVPN – genericTrap : enterpriseSpecific – specific-trap : FL MGUARDTrapVPNIKEServerStatus (1) – additional : FL MGUARDTResVPNStatus
		This trap is sent when the IPsec IKE server is started or stopped.
		– enterprise-oid : FL MGUARDTrapVPN – genericTrap : enterpriseSpecific – specific-trap : FL MGUARDTrapVPNIPsecConnStatus (2) – additional : FL MGUARDTResVPNName, FL MGUARDTResVPNIndex, FL MGUARDTResVPNPeer, FL MGUARDTResVPNStatus, FL MGUARDTResVPNType, FL MGUARDTResVPNLocal, FL MGUARDTResVPNRemote
		This trap is sent when the status of an IPsec connection changes.
		– enterprise-oid : FL MGUARD – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapVPNIPsecConnStatus
		This trap is sent when a connection is established or aborted. It is not sent when the FL MGUARD is about to accept a connection request for this connection.
	L2TP connection status changes	Activate traps **Yes/No**
		– enterprise-oid : FL MGUARDTrapVPN – genericTrap : enterpriseSpecific – specific-trap : FL MGUARDTrapVPNL2TPConnStatus (3) – additional : FL MGUARDTResVPNName, FL MGUARDTResVPNIndex, FL MGUARDTResVPNPeer, FL MGUARDTResVPNStatus, FL MGUARDTResVPNLocal, FL MGUARDTResVPNRemote
		This trap is sent when the status of an L2TP connection changes.
Trap destinations	**Traps can be sent to multiple destinations.**	
	Destination IP	IP address to which the trap should be sent.

Management >> SNMP >> Trap [...]		
	Destination Port	Standard: 162
		Destination port to which the trap should be sent.
	Destination Name	Optional name for the destination. Does not affect the generated traps.
	Destination Community	Name of the SNMP community to which the trap is assigned.

5.2.6.3   LLDP

LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) uses suitable request methods to automatically determine the (Ethernet) network infrastructure. LLDP-capable devices periodically send Ethernet multicasts (layer 2). Tables of systems connected to the network are created from the responses, and these can be requested via SNMP.

Management >> SNMP >> LLDP		
LLDP	**Mode**	**Enabled/Disabled**
		The LLDP service or agent can be globally enabled or disabled here. If the function is enabled, this is indicated by a green signal field on the tab at the top of the page. If the signal field is red, the function is disabled.
Internal/LAN interface **External/WAN interface**	**Chassis ID**	A unique ID of the computer found; typically one of its MAC addresses.
	IP address	IP address of the computer found. This can be used to perform administrative activities on the computer via SNMP.
	Port description	A textual description of the network interface where the computer was found.
	System name	Host name of the computer found.
	Button: Update	To update the displayed data, if necessary, click on **Update**.

5.2.7 Management >> Central Management

5.2.7.1 Configuration Pull

The FL MGUARD can retrieve new configuration profiles from an HTTPS server in adjustable time intervals, provided that the server makes them available to the FL MGUARD as files (file extension: .atv). If the configuration provided differs from the active configuration of the FL MGUARD, the available configuration is automatically downloaded and activated.

Management >> Central Management >> Configuration Pull		
Configuration Pull	**Pull Schedule**	Here, specify whether (and if so, when and at what intervals) the FL MGUARD should attempt to download and apply a new configuration from the server. To do this, open the selection list and select the desired value.
		A new field is shown when **Time Schedule** is selected. In this field, specify whether the new configuration should be downloaded from the server daily or regularly on a certain weekday, and at what time.
		Time-controlled download of a new configuration is only possible if the system time has been synchronized (see "Management >> System Settings" on page 50, "Time and Date" on page 53).
		Time control sets the selected time based on the configured time zone.
	Server	IP address or host name of the server that provides the configurations.

Management >> Central Management >> Configuration Pull [...]		
	Directory	The directory (folder) on the server where the configuration is located.
	Filename	The name of the file in the directory defined above. If no file name is defined here, the serial number of the FL MGUARD is used with file extension ".atv".
	Number of times a configuration profile is ignored after it was rolled back	Standard: 10
		After retrieving a new configuration, it is possible that the FL MGUARD may no longer be accessible after applying the new configuration. It is then no longer possible to implement a new remote configuration to make corrections. In order to prevent this, the FL MGUARD performs the following check:

As soon as the retrieved configuration is applied, the FL MGUARD tries to connect to the configuration server again based on the new configuration. The FL MGUARD then attempts to download the newly applied configuration profile again.

If successful, the new configuration remains in effect.

If this check is unsuccessful for whatever reason, the FL MGUARD assumes that the newly applied configuration profile is faulty. The FL MGUARD remembers the MD5 total for identification purposes. It then performs a rollback.

Rollback means that the last (working) configuration is restored. This assumes that the new (non-functioning) configuration contains an instruction to perform a rollback if a newly loaded configuration profile is found to be faulty according to the checking procedure described above.

When the FL MGUARD makes subsequent attempts to retrieve a new configuration profile periodically after the time defined in the **Pull Schedule** field (and **Time Schedule**) has elapsed, it will only accept the profile subject to the following selection criterion: The configuration profile provided **must differ** from the configuration profile previously identified as faulty for the FL MGUARD and which resulted in the rollback.

(The FL MGUARD checks the MD5 total stored for the old, faulty, and rejected configuration against the MD5 total of the new configuration profile offered.)

If this selection criterion is **met**, i.e., a newer configuration profile is offered, the FL MGUARD retrieves this configuration profile, applies it, and checks it according to the procedure described above. It also disables the configuration profile by means of rollback if the check is unsuccessful.

If the selection criterion is **not met** (i.e., the same configuration profile is being offered), the selection criterion remains in force for all further cyclic requests for the period specified in the **Number of times...** field.

If the specified number of times elapses without a change of the configuration profile on the configuration server, the FL MGUARD applies the unchanged new ("faulty") configuration profile again, despite it being "faulty". This is to rule out the possibility that external factors (e.g., network failure) may have resulted in the check being unsuccessful.

The FL MGUARD then attempts to connect to the configuration server again based on the new configuration that has been reapplied. It then attempts to download the newly applied configuration profile again. If this is unsuccessful, another rollback is performed. The selection criterion is enforced again for the further cycles for loading a new configuration as often as is defined in the **Number of times...** field.

Management >> Central Management >> Configuration Pull [...]	
	If the value in the **Number of times...** field is specified as **0**, the selection criterion will never be enforced (the offered configuration profile is ignored if it remains unchanged). As a result, the second of the following objectives could then no longer be met.
	This mechanism has the following objectives:
	1. After applying a new configuration, it must be ensured that the FL MGUARD can still be configured from a remote location.
	2. When cycles are close together (e.g., **Pull Schedule** = 15 minutes), the FL MGUARD must be prevented from repeatedly testing a configuration profile that might be faulty at intervals that are too short. This can hinder or prevent external administrative access, as the FL MGUARD might be too busy dealing with its own processes.
	3. External factors (e.g., network failure) must be largely ruled out as a reason why the FL MGUARD considers the new configuration to be faulty. .
	ℹ An application note is provided by Innominate. It describes how a rollback can be started using a configuration profile. (Application notes are available in the download area at innominate.com.)
Download timeout (seconds)	Default: 120.
	Specifies the maximum timeout length (period of inactivity) when downloading the configuration file. The download is aborted if this time is exceeded. If and when a new download is attempted depends on the setting of *Pull Schedule* (see above).
Login	Login (user name) that the HTTPS server requests.
Password	Password that the HTTPS server requests.
Server Certificate	The certificate that the FL MGUARD uses to check the authenticity of the certificate "shown" by the configuration server. It prevents an incorrect configuration from an unauthorized server from being installed on the FL MGUARD.
	The following may be specified here:
	– A self-signed certificate of the configuration server.
	– The root certificate of the CA (certification authority) that issued the server certificate. This is valid when the configuration server certificate is signed by a CA (instead of self-signed).

Management >> Central Management >> Configuration Pull [...]

		ℹ If the stored configuration profiles also contain the private VPN key for the VPN connection(s) with PSK, the following conditions must be met:
		– The password should consist of at least 30 random upper and lower case letters and numbers (to prevent unauthorized access).
		– The HTTPS server should only grant access to the configuration of this individual FL MGUARD using the login and password specified. Otherwise, users of other FL MGUARD devices could access this individual FL MGUARD.
		ℹ The IP address or the host name specified under Server must be the same as the server certificate's common name (CN).
		Self-signed certificates should not use the "key-usage" extension.
		To install a certificate, proceed as follows:
		Requirement: The certificate file must be saved on the connected computer.
		• Click on **Browse...** to select the file.
		• Click on **Import**.
	Download Test	• By clicking on **Test Download**, you can test whether the specified parameters are correct without actually saving the modified parameters or activating the configuration profile. The result of the test is displayed in the right-hand column.
		ℹ Ensure that the profile on the server does not contain unwanted variables starting with "GAI_PULL_", as these overwrite the applied configuration.

5.2.8   Management >> Restart

5.2.8.1   Restart
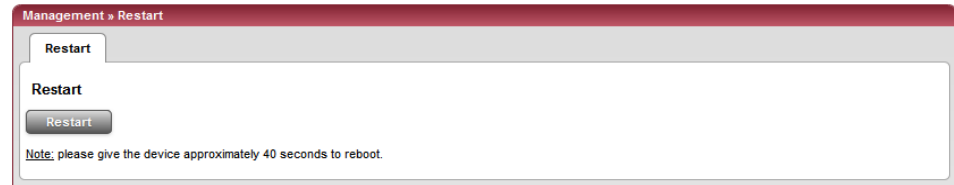
Restarts the FL MGUARD. Has the same effect as a temporary interruption in the power supply, whereby the FL MGUARD is switched off and on again.

A restart (reboot) is necessary in the event of an error. It may also be necessary after a software update.

5.3   Network menu

5.3.1   Network >> Interfaces

The FL MGUARD has the following interfaces with external access:

	Ethernet: Internal: LAN External: WAN	Serial interface	Built-in modem	Serial console via USB[1]
FL MGUARD SMART2	**Yes**	**No**	**No**	**Yes**
FL MGUARD RS4000/RS2000, FL MGUARD PCI4000, FL MGUARD DELTA TX/TX,	**Yes**	**Yes**	**No**	**No**

[1]   See "Serial console via USB" on page 139

The LAN port is connected to a single computer or the local network (internal). The WAN port is used to connect to the external network. For devices with a serial interface, the connection to the external network can also or additionally be established via the serial interface using a modem. Alternatively, the serial interface can also be used as follows: For PPP dial-in into the local network or for configuration purposes. For devices with a built-in modem (analog modem or ISDN terminal adapter), the modem can be used additionally to combine access options.

The details for this must be configured on the *General, Ethernet, Dial-out, Dial-in*, and *Modem/Console* tab pages. For a more detailed explanation of the options for using the serial interface (and a built-in modem), see "Modem/Console" on page 138.

5.3.1.1 General

Network >> Interfaces >> General		
Network Status	**External IP address (WAN port address)**	Display only: The addresses via which the FL MGUARD can be accessed by devices from the external network. They form the interface to other parts of the LAN or to the Internet. If the transition to the Internet takes place here, the IP addresses are usually assigned by the Internet service provider (ISP). If an IP address is assigned dynamically to the FL MGUARD, the currently valid IP address can be found here.
		In *Stealth* mode, the FL MGUARD adopts the address of the locally connected computer as its external IP.
	Network Mode status	Displays the status of the selected network mode.
	Active Defaultroute	Display only: The IP address that the FL MGUARD uses to try to reach unknown networks is displayed here. This field can contain "none" if the FL MGUARD is in *Stealth* mode.
	Used DNS servers	Display only: The names of the DNS servers used by the FL MGUARD for name resolution are displayed here. This information can be useful, for example, if the FL MGUARD is using the DNS servers assigned to it by the Internet service provider.

Network >> Interfaces >> General [...]		
Network Mode	**Network Mode**	**Stealth/Router**
		The FL MGUARD must be set to the network mode that corresponds to its connection to the network.
		Depending on which network mode the FL MGUARD is set to, the page will change together with its configuration parameters.
		See:
		"Stealth (default settings for FL MGUARD RS4000/RS2000, FL MGUARD SMART2, FL MGUARD PCI4000, FL MGUARD DELTA TX/TX)" on page 107 and "Network Mode: Stealth" on page 111
		"Router" on page 108 and "Network Mode: Router" on page 122
Router Mode	Only used when "Router" is selected as the network mode.	**Static/DHCP/PPPoE/PPTP/Modem[1]**
		See:
		"Router Mode: static" on page 109 and ""Router" network mode, "PPTP" router mode" on page 127
		"Router Mode: DHCP" on page 109 and ""Router" network mode, "DHCP" router mode" on page 125
		"Router Mode: PPPoE" on page 109 and ""Router" network mode, "PPPoE" router mode" on page 126
		"Router Mode: PPTP" on page 109 and ""Router" network mode, "PPTP" router mode" on page 127
		"Router Mode: Modem" on page 110 and ""Router" network mode, "Modem/Built-in Modem" router mode" on page 128
		""Router" network mode, "Modem/Built-in Modem" router mode" on page 128

[1]   *Modem* is not available for all FL MGUARD models (see "Network >> Interfaces" on page 104).

Stealth (default settings for FL MGUARD RS4000/RS2000, FL MGUARD SMART2, FL MGUARD PCI4000, FL MGUARD DELTA TX/TX)

Stealth mode is used to protect a single computer or a local network with the FL MGUARD. Important: If the FL MGUARD is in *Stealth* network mode, it is inserted into the existing network (see figure) without changing the existing network configuration of the connected devices.

Before:

After:
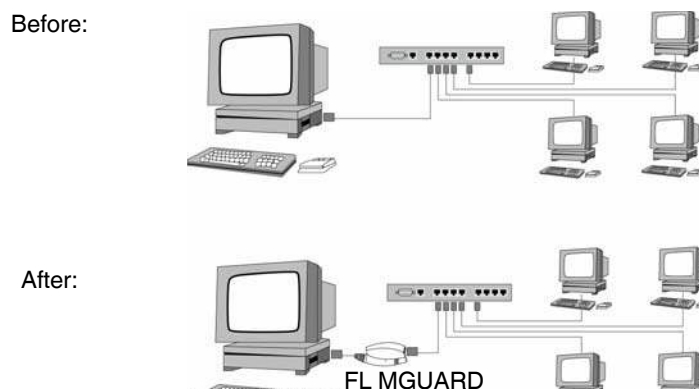
FL MGUARD

(A LAN can also be on the left.)

The FL MGUARD analyzes the active network traffic and independently configures its network connection accordingly. It then operates transparently, i.e., without the computers having to be reconfigured.

As in the other modes, firewall and VPN security functions are available.

Externally supplied DHCP data is allowed through to the connected computer.

> ℹ️ If the FL MGUARD is to provide services such as VPN, DNS, NTP, etc., a firewall installed on the computer must be configured to allow ICMP echo requests (ping).

> ℹ️ In *Stealth* mode, the FL MGUARD uses internal IP address 1.1.1.1. This can be accessed from the computer if the default gateway configured on the computer is accessible.

In *Stealth* network mode, a secondary external interface can also be configured (see "Secondary External Interface" on page 115).

For the further configuration of *Stealth* network mode, see "Network Mode: Stealth" on page 111.

Router

If the FL MGUARD is in *Router* mode, it acts as the gateway between various subnetworks and has both an external interface (WAN port) and an internal interface (LAN port) with at least one IP address.

WAN port

The FL MGUARD is connected to the Internet or other "external" parts of the LAN via its WAN port.
– FL MGUARD SMART2: The WAN port is the Ethernet socket.

LAN port

The FL MGUARD is connected to a local network or a single computer via its LAN port.
– FL MGUARD SMART2: The LAN port is the Ethernet connector.
    In *Power-over-PCI mode*, the LAN port is the LAN socket of the FLMGUARD PCI4000.

As in the other modes, firewall and VPN security functions are available.

> **i** If the FL MGUARD is operated in *Router* mode, it must be set as the default gateway on the locally connected computers.
>
> This means that the IP address of the FL MGUARD LAN port must be specified as the default gateway address on these computers.

> **i** NAT should be activated if the FL MGUARD is operated in *Router* mode and establishes the connection to the Internet (see "Network >> NAT" on page 142).
>
> Only then can the computers in the connected local network access the Internet via the FL MGUARD. If NAT is not activated, it is possible that only VPN connections can be used.

In *Router* network mode, a secondary external interface can also be configured (see "Secondary External Interface" on page 115).

There are several Router modes, depending on the Internet connection:
– Static
– DHCP
– PPPoE
– PPPT
– Modem

Router Mode: static

The IP address is fixed.

Router Mode: DHCP

The IP address is assigned via DHCP.

Router Mode: PPPoE

PPPoE mode corresponds to Router mode with DHCP but with one difference: The PPPoE protocol, which is used by many DSL modems (for DSL Internet access), is used to connect to the external network (Internet, WAN). The external IP address, which the FL MGUARD uses for access from remote partners, is specified by the provider.

i	If the FL MGUARD is operated in *PPPoE* mode, the FL MGUARD must be set as the default gateway on the locally connected computers. This means that the IP address of the FL MGUARD LAN port must be specified as the default gateway address on these computers.

i	If the FL MGUARD is operated in *PPPoE* mode, NAT must be activated in order to gain access to the Internet. If NAT is not activated, it is possible that only VPN connections can be used.

For the further configuration of *PPPoE* network mode, see ""Router" network mode, "PPPoE" router mode" on page 126.

Router Mode: PPTP

Similar to *PPPoE* mode. For example, in Austria the PPTP protocol is used instead of the PPPoE protocol for DSL connections.

(PPTP is the protocol that was originally used by Microsoft for VPN connections.)

i	If the FL MGUARD is operated in *PPTP* mode, the FL MGUARD must be set as the default gateway on the locally connected computers. This means that the IP address of the FL MGUARD LAN port must be specified as the default gateway on these computers.

i	If the FL MGUARD is operated in *PPTP* mode, NAT should be activated in order to gain access to the Internet from the local network (see "Network >> NAT" on page 142). If NAT is not activated, it is possible that only VPN connections can be used.

For the further configuration of *PPTP* network mode, see ""Router" network mode, "PPTP" router mode" on page 127.

Router Mode: Modem

| **i** | Only used for *FL MGUARD industrial rs* **without** built-in modem, *FL MGUARD RS4000*, FL MGUARD DELTA TX/TX. |

If *Modem* network mode is selected, the external Ethernet interface of the FL MGUARD is deactivated and data traffic is transferred to and from the WAN via the externally accessible serial interface (serial port) of the FL MGUARD.

An external modem, which establishes the connection to the telephone network, is connected to the serial port. The connection to the WAN or Internet is then established via the telephone network (by means of the external modem).

| **i** | If the address of the FL MGUARD is changed (e.g., by changing the network mode from *Stealth* to *Router*), the device can only be accessed via the new address. If the configuration is changed via the LAN port, confirmation of the new address is displayed before the change is applied. If configuration changes are made via the WAN port, no confirmation is displayed. |

| **i** | If the mode is set to *Router*, *PPPoE* or *PPTP* and you then change the IP address of the LAN port and/or the local subnet mask, make sure you specify the correct values. Otherwise, the FL MGUARD may no longer be accessible under certain circumstances.

For the further configuration of *Built-in Modem/Modem* network mode, see ""Router" network mode, "Modem/Built-in Modem" router mode" on page 128. |

Network Mode: Stealth

ℹ	Default settings for FL MGUARD RS4000/RS2000, FL MGUARD SMART2, FL MGUARD PCI4000, FL MGUARD DELTA TX/TX.

When "Stealth" is selected as the network mode...

... and "static" is selected for the Stealth

Network >> Interfaces >> General ("Stealth" network mode)

Network Mode

ℹ	Only applies if "Stealth" is selected as the network mode.

Stealth configuration   **autodetect/static/multiple clients**

autodetect

The FL MGUARD analyzes the network traffic and independently configures its network connection accordingly. It operates transparently.

Network >> Interfaces >> General ("Stealth" network mode) [...]		
		static
		If the FL MGUARD cannot analyze the network traffic, e.g., because the locally connected computer only receives data and does not send it, then *Stealth configuration* must be set to **static**. In this case, further entry fields are available for the Static Stealth Configuration at the bottom of the page.
		multiple clients
		(Default) As with **autodetect**, but it is possible to connect more than one computer to the LAN port (secure port) of the FL MGUARD, meaning that multiple IP addresses can be used at the LAN port (secure port) of the FL MGUARD.
	Autodetect: ignore NetBIOS over TCP traffic on TCP port 139	**No/Yes**
		Only with autodetect stealth configuration: If a Windows computer has more than one network card installed, it may alternate between the different IP addresses for the sender address in the data packets it sends. This applies to network packets that the computer sends to TCP port 139 (NetBIOS). As the FL MGUARD determines the address of the computer from the sender address (and thus the address via which the FL MGUARD can be accessed), the FL MGUARD would have to switch back and forth, and this would hinder operation considerably. To avoid this, set this option to **Yes** if the FL MGUARD has been connected to a computer that has these properties.

Network >> Interfaces >> General ("Stealth" network mode) [...]

Stealth Management IP Address	

Management IP addresses		IP	Netmask	Use VLAN	VLAN ID
	⬇✕	192.168.11.1	255.255.255.0	No ▼	1
	⬇☐	192.168.5.1	255.255.255.0	No ▼	1
Default gateway	192.168.11.10				

An additional IP address can be specified here for the administration of the FL MGUARD.

If

–   The multiple clients option is selected under *Stealth configuration*

–   The client does not answer ARP requests

–   No client is available

Remote access via HTTPS, SNMP, and SSH is **only** possible using this address.

> **ℹ** With *static* Stealth configuration, the *Stealth Management IP Address* can always be accessed, even if the network card of the client PC has not been activated.

> **ℹ** If the secondary external interface is activated (see "Secondary External Interface" on page 115), the following applies:
>
> If the routing settings are such that data traffic to the **Stealth Management IP Address** would be routed via the secondary external interface, this would be an exclusion situation, i.e., the FL MGUARD could no longer be administered locally.
>
> To prevent this, the FL MGUARD has a built-in mechanism that ensures that in such an event the Stealth Management IP Address can still be accessed by the locally connected computer (or network).

Network >> Interfaces >> General ("Stealth" network mode) [...]		
	Management IP addresses	**IP**
		IP address via which the FL MGUARD can be accessed and administered.
		The IP address "0.0.0.0" deactivates the management IP address.
		Change the management IP address first before specifying any additional addresses.
		Netmask
		The subnet mask of the IP address above.
		Use VLAN: Yes/No
		IP address and subnet mask of the VLAN port.
		If the IP address should be within a VLAN, set this option to **Yes**.
		VLAN ID
		– A VLAN ID between 1 and 4095.
		– If you want to delete entries from the list, please note that the first entry cannot be deleted.
		ⓘ In multi stealth mode, the external DHCP server of the FL MGUARD cannot be used if a VLAN ID is assigned as the management IP.
	Default gateway	The default gateway of the network where the FL MGUARD is located.
Static routes	In Stealth modes "autodetect" and "static", the FL MGUARD adopts the default gateway of the computer connected to its LAN port. This does not apply if a management IP address is configured with the default gateway.	
	Alternative routes can be specified for data packets destined for the WAN that have been created by the FL MGUARD. These include the packets from the following types of data traffic:	
	– Download of certificate revocation lists (CRLs)	
	– Download of a new configuration	
	– Communication with an NTP server (for time synchronization)	
	– Sending and receiving encrypted data packets from VPN connections	
	– Requests to DNS servers	
	– Syslog messages	
	– Download of firmware updates	
	– Download of configuration profiles from a central server (if configured)	
	– SNMP traps	
	If this option is used, make the relevant entries afterwards. If it is not used, the affected data packets are routed via the default gateway specified for the client.	
	Networks to be routed over alternative gateways Network Gateway	

Network >> Interfaces >> General ("Stealth" network mode) [...]			
	Network	Specify the network in CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).	
	Gateway	The gateway via which this network can be accessed.	
		The routes specified here are mandatory routes for data packets created by the FL MGUARD. This setting has priority over other settings (see also "Network example diagram" on page 295).	
Static Stealth Configuration	**Client's IP address**	The IP address of the computer connected to the LAN port.	
	Client's MAC address	The physical address of the network card of the local computer to which FL MGUARD is connected.	
		• The MAC address can be determined as follows:	
		In DOS (Start, Programs, Accessories, Command Prompt), enter the following command: ***ipconfig /all***	

The MAC address does not necessarily have to be specified. The FL MGUARD can automatically obtain the MAC address from the client. The MAC address 0:0:0:0:0:0 must be set in order to do this. Please note that the FL MGUARD can only forward network packets to the client once the MAC address of the client has been determined.

If no *Stealth Management IP Address* or *Client's MAC address* is configured in static Stealth mode, then DAD ARP requests are sent via the internal interface (see RFC 2131, Section 4.4.1).

Secondary External Interface

This menu item is not included in the scope of functions for the FL MGUARD RS2000.

ℹ	Only in *Router* network mode **with** *static* router mode or *Stealth* network mode. *FL MGUARD RS4000* only
	In these network modes, the serial interface of the FL MGUARD can be configured as an additional **Secondary External Interface**.

The secondary external interface can be used to transfer data traffic *permanently* or *temporarily* to the external network (WAN).

If the secondary external interface is activated, the following applies:

In *Stealth* **network mode**

Only the data traffic generated by the FL MGUARD is subject to the routing specified for the secondary external interface, not the data traffic from a locally connected computer. Locally connected computers cannot be accessed remotely either; only the FL MGUARD itself can be accessed remotely – if the configuration permits this.

As in Router network mode, VPN data traffic can flow to and from the locally connected computers. Because this traffic is encrypted by the FL MGUARD, it is seen as being generated by the FL MGUARD.

In *Router* **network mode**

All data traffic, i.e., from and to locally connected computers, generated by the FL MGUARD, can be routed to the external network (WAN) via the secondary external interface.

Network >> Interfaces >> General ("Stealth" network mode) [...]

Secondary External Interface

Network Mode Off ▼

Network Mode: Off/Modem

Off

(Default). Select this setting if the operating environment of the FL MGUARD does not require a secondary external interface. You can then use the serial interface (or the built-in modem, if present) for other purposes (see "Modem/Console" on page 138).

Modem/Built-in Modem

If you select one of these options, the secondary external interface will be used to route data traffic *permanently* or *temporarily* to the external network (WAN).

The secondary external interface is created via the serial interface of the FL MGUARD and an external modem connected to it.

Operation Mode **permanent/temporary**

After selecting *Modem* or *Built-in Modem* network mode for the secondary external interface, the operating mode of the secondary external interface must be specified.

Secondary External Interface

Network Mode	Modem ▼	
Operation Mode	permanent ▼	
Secondary External Routes	**Network**	**Gateway**
	192.168.3.0/24	%gateway

permanent

Data packets whose destination corresponds to the routing settings specified for the secondary external interface are always routed via this external interface. The secondary external interface is always activated.

temporary

Data packets whose destination corresponds to the routing settings specified for the secondary external interface are only routed via this external interface when additional, separately defined conditions are met. Only then is the secondary external interface activated and the routing settings for the secondary external interface take effect (see "Probes for Activation" on page 119).

Network >> Interfaces >> General ("Stealth" network mode) [...]

	Secondary External Routes	**Network**
		Specify the routing to the external network here. Multiple routes can be specified. Data packets intended for these networks are then routed to the corresponding network via the secondary external interface – in *permanent* or *temporary* mode.
		Gateway
		Specify the IP address (if known) of the gateway that is used for routing to the external network described above.
		When you dial into the Internet using the phone number of the Internet service provider, the address of the gateway is usually not known until you have dialed in. In this case, enter **%gateway** in the field as a wildcard.

Operation Mode: permanent/temporary

In both **permanent** and **temporary** operating mode, the modem must be available to the FL MGUARD for the secondary external interface so that the FL MGUARD can establish a connection to the WAN (Internet) via the telephone network connected to the modem.

Which data packets are routed via the **primary external interface** (Ethernet interface) and which data packets are routed via the **secondary external interface** is determined by the routing settings that are applied for these two external interfaces. Therefore an interface can only take a data packet if the routing setting for that interface matches the destination of the data packet.

The following rules apply for routing entries:

If multiple routing entries for the destination of a data packet match, then the smallest network defined in the routing entries that matches the data packet destination determines which route this packet takes.

Example:

– The external route of the **primary** external interface is specified as 10.0.0.0/8, while the external route of the **secondary** external interface is specified as 10.1.7.0/24. Data packets to network 10.1.7.0/24 are then routed via the secondary external interface, although the routing entry for the primary external interface also matches them. Explanation: The routing entry for the secondary external interface refers to a smaller network (10.1.7.0/24 < 10.0.0.0/8).
– This rule does not apply in *Stealth* network mode with regard to the stealth management IP address (see note under "Stealth Management IP Address" on page 113).
– If the routing entries for the primary and secondary external interfaces are identical, then the secondary external interface "wins", i.e., the data packets with a matching destination address are routed via the secondary external interface.
– The routing settings for the secondary external interface only take effect when the secondary external interface is activated. Particular attention must be paid to this if the routing entries for the primary and secondary external interfaces overlap or are identical, whereby the priority of the secondary external interface has a filter effect, with the following result: Data packets whose destination matches both the primary and secondary external interfaces are always routed via the secondary external interface, but only if this is activated.
– In **temporary** mode, "activated" signifies the following: The secondary external interface is only activated when specific conditions are met, and it is only then that the routing settings of the secondary external interface take effect.
– Network address 0.0.0.0/0 generally refers to the largest definable network, i.e., the Internet.

> **i** In Router network mode, the local network connected to the FL MGUARD can be accessed via the secondary external interface as long as the specified firewall settings allow this.

Network >> Interfaces >> General (continued); Secondary External Interface (continued)

Secondary External Interface (continued)	**Probes for Activation**

Network Mode = Modem

Operation Mode = temporary

Network Mode	Modem ▾
Operation Mode	temporary ▾

Secondary External Routes	Network	Gateway
	192.168.3.0/24	%gateway

Probes for Activation
(The secondary external interface is activated only if *all* probes fail, and if the operation mode is set to "temporary".)

	Type	Destination	Comment

Probe Interval (seconds)	20
Number of times all probes need to fail during subsequent runs before the secondary external interface is activated.	2
DNS Mode	use primary DNS settings untouched ▾

User defined name servers
(If they should be reachable via the secondary external interface please configure a route for them.)

IP

If the operating mode of the secondary external interface is set to **temporary**, the following is checked using periodic ping tests: Can a specific destination or destinations be reached when data packets take the route based on all the routing settings specified for the FL MGUARD – apart from those specified for the secondary external interface? Only if **none** of the ping tests are successful does the FL MGUARD assume that it is currently not possible to reach the destination(s) via the primary external interface (Ethernet interface or WAN port of the FL MGUARD). In this case, the secondary external interface is activated, which results in the data packets being routed via this interface (according to the routing setting for the secondary external interface).

The secondary external interface remains activated until the FL MGUARD detects in subsequent ping tests that the destination(s) can be reached again. If this condition is met, the data packets are routed via the **primary** external interface again and the **secondary** external interface is deactivated.

Therefore, the purpose of the ongoing ping tests is to check whether specific destinations can be reached via the primary external interface. When they cannot be reached, the secondary external interface is activated until they can be reached again.

Type/Destination

Specify the ping **Type** of the ping request packet that the FL MGUARD is to send to the device with the IP address specified under **Destination**.

Multiple ping tests can be configured for different destinations.

Success/failure:

A ping test is successful if the FL MGUARD receives a positive response to the sent ping request packet within 4 seconds. If the response is positive, the partner can be reached.

Network >> Interfaces >> General (continued); Secondary External Interface (continued)		
		Ping types:
		– IKE ping:
		Determines whether a VPN gateway can be reached at the IP address specified.
		– ICMP ping:
		Determines whether a device can be reached at the IP address specified.
		This is the most common ping test. However, the response to this ping test is disabled on some devices. This means that they do not respond even though they can be reached.
		– DNS ping:
		Determines whether an operational DNS server can be reached at the IP address specified.
		A generic request is sent to the DNS server with the specified IP address, and every DNS server that can be reached responds to this request.
		Please note the following when programming ping tests:
		It is useful to program multiple ping tests. This is because it is possible that an individual tested service is currently undergoing maintenance. This type of scenario should not result in the secondary external interface being activated and an expensive dial-up line connection being established via the telephone network.
		Because the ping tests generate network traffic, the number of tests and their frequency should be kept within reasonable limits. You should also avoid activating the secondary external interface too early. The timeout time for the individual ping requests is 4 seconds. This means that after a ping test is started, the next ping test starts after 4 seconds if the previous one was unsuccessful.
		To take these considerations into account, make the following settings.
	Probe Interval (seconds)	The ping tests defined above under **Probes for Activation...** are performed one after the other. When the ping tests defined are performed once in sequence, this is known as a *test run*. Test runs are continuously repeated at intervals. The interval entered in this field specifies how long the FL MGUARD waits after starting a test run before it starts the next test run. The test runs are not necessarily completed: As soon as one ping test in a test run is successful, the subsequent ping tests in this test run are omitted. If a test run takes longer than the interval specified, then the subsequent test run is started directly after it.

Network >> Interfaces >> General (continued); Secondary External Interface (continued)		
	Number of times all probes need to fail during subsequent runs before the secondary external interface is activated	Specifies how many sequentially performed test runs must return a negative result before the FL MGUARD activates the secondary external interface. The result of a test run is negative if **none** of the ping tests it contains were successful.
		The number specified here also indicates how many consecutive test runs must be successful after the secondary external interface has been activated before this interface is deactivated again.
	DNS Mode	Only relevant if the secondary external interface is activated in **temporary** mode:
		The DNS mode selected here specifies which DNS server the FL MGUARD uses for temporary connections established via the secondary external interface.
		– Use primary DNS settings untouched
		– DNS Root Servers
		– Provider defined (via PPP dial-up)
		– User defined (servers listed below)
		Use primary DNS settings untouched
		The DNS servers defined under Network --> DNS Server (see "Network >> NAT" on page 142) are used.
		DNS Root Servers
		Requests are sent to the root name servers on the Internet whose IP addresses are stored on the FL MGUARD. These addresses rarely change.
		Provider defined (via PPP dial-up)
		The domain name servers of the Internet service provider that provide access to the Internet are used.
		User defined (servers listed below)
		If this setting is selected, the FL MGUARD will connect to the domain name servers listed under *User defined name servers*.
	User defined name servers	The IP addresses of domain name servers can be entered in this list. The FL MGUARD uses this list for communication via the secondary external interface – as long as the interface is activated temporarily and *User defined* is specified under **DNS Mode** (see above) in this case.

Network Mode: Router

When "Router" is
selected as the network
mode and "static" is
selected as the Router
mode (see Page 124)

Network >> Interfaces >> General ("Router" network mode)		
Internal Networks	**Internal IPs (trusted port)**	The internal IP is the IP address via which the FL MGUARD can be accessed by devices in the locally connected network.
		The default settings in **Router/PPPoE/PPTP/Modem** mode are as follows:
		– IP address: **192.168.1.1**
		– Netmask: **255.255.255.0**
		You can also specify other addresses via which the FL MGUARD can be accessed by devices in the locally connected network. For example, this can be useful if the locally connected network is divided into subnetworks. Multiple devices in different subnetworks can then access the FL MGUARD via different addresses.
	IP	IP address via which the FL MGUARD can be accessed via its LAN port.
	Netmask	The subnet mask of the network connected to the LAN port.
	Use VLAN	If the IP address should be within a VLAN, set this option to **Yes**.
	VLAN ID	– A VLAN ID between 1 and 4095.
		– If you want to delete entries from the list, please note that the first entry cannot be deleted.

Network >> Interfaces >> General ("Router" network mode) [...]		
	Additional Internal Routes	Additional routes can be defined if further subnetworks are connected to the locally connected network.
	Network	Specify the network in CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
	Gateway	The gateway via which this network can be accessed.
		See also "Network example diagram" on page 295).
Secondary External Interface	See "Secondary External Interface" on page 115	

"Router" network mode, "static" router mode

Network >> Interfaces >> General ("Router" network mode, "static" router mode)		
External Networks	**External IPs (untrusted port)**	The addresses via which the FL MGUARD can be accessed by devices on the WAN port side. If the transition to the Internet takes place here, the external IP address of the FL MGUARD is assigned by the Internet service provider (ISP).
		IP/Netmask
		– IP address and subnet mask of the WAN port.
		Use VLAN: Yes/No
		– If the IP address should be within a VLAN, set this option to Yes.
		VLAN ID
		– A VLAN ID between 1 and 4095.
		– If you want to delete entries from the list, please note that the first entry cannot be deleted.
	Additional External Routes	In addition to the default route via the default gateway specified below, additional external routes can be specified.
		Network/Gateway
		(See "Network example diagram" on page 295)

Network >> Interfaces >> General ("Router" network mode, "static" router mode)		
	IP of default gateway	The IP address of a device in the local network (connected to the LAN port) or the IP address of a device in the external network (connected to the WAN port) can be specified here.
		If the FL MGUARD establishes the transition to the Internet, this IP address is assigned by the Internet service provider (ISP).
		If the FL MGUARD is used within the LAN, the IP address of the default gateway is assigned by the network administrator.
		If the local network is not known to the external router, e.g., in the event of configuration via DHCP, specify your local network under Network >> NAT (see Page 142).
Internal Networks	See "Internal Networks" on page 122	
Secondary External Interface	See "Secondary External Interface" on page 115	

"Router" network mode, "DHCP" router mode

There are no additional setting options for "Router" network mode, "DHCP" router mode.

Network >> Interfaces >> General ("Router" network mode, "DHCP" router mode)	
Internal Networks	See "Internal Networks" on page 122
Secondary External Interface	See "Secondary External Interface" on page 115

"Router" network mode, "PPPoE" router mode

When "Router" is selected as the network mode and "PPPoE" is selected as the router mode

Network >> Interfaces >> General ("Router" network mode, "PPPoE" router mode)		
PPPoE	**For access to the Internet, the Internet service provider (ISP) provides the user with a user name (login) and password. These are requested when you attempt to establish a connection to the Internet.**	
	PPPoE Login	The user name (login) that is required by the Internet service provider (ISP) when you attempt to establish a connection to the Internet.
	PPPoE Password	The password that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	Request PPPoE Service Name?	When **Yes** is selected, the PPPoE client of the FL MGUARD requests the service name specified below from the PPPoE server. Otherwise, the PPPoE service name is not used.
	PPPoE Service Name	PPPoE service name
	Automatic Re-connect?	If **Yes** is selected, specify the time in the **Re-connect daily at** field. This feature is used to schedule Internet disconnection and reconnection (as required by many Internet service providers) so that they do not interrupt normal business operations.
		When this function is enabled, it only takes effect if synchronization with a time server has been carried out (see "Management >> System Settings" on page 50, "Time and Date" on page 53).
	Re-connect daily at	Specified time at which the *Automatic Re-connect* function (see above) should be performed.
Internal Networks	See "Internal Networks" on page 122	
Secondary External Interface	See "Secondary External Interface" on page 115	

"Router" network mode, "PPTP" router mode

When "Router" is selected as the network mode and "PPTP" is selected as the router mode

Network >> Interfaces >> General ("Router" network mode, "PPTP" router mode)		
PPTP	**For access to the Internet, the Internet service provider (ISP) provides the user with a user name (login) and password. These are requested when you attempt to establish a connection to the Internet.**	
	PPTP Login	The user name (login) that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	PPTP Password	The password that is required by the Internet service provider when you attempt to establish a connection to the Internet.
	Local IP Mode	**Via DHCP:** If the address data for access to the PPTP server is provided by the Internet service provider via DHCP, select **Via DHCP**. In this case, no entry is required under **Local IP**. **Static (from field below):** If the address data for access to the PPTP server is **not** supplied by the Internet service provider via DHCP, the local IP address must be specified.
	Local IP	The IP address via which the FL MGUARD can be accessed by the PPTP server.
	Modem IP	The address of the PPTP server of the Internet service provider.
Internal Networks	See "Internal Networks" on page 122	
Secondary External Interface This menu item is not included in the scope of functions for the FL MGUARD RS2000.	See "Secondary External Interface" on page 115	

"Router" network mode, "Modem/Built-in Modem" router mode

i	*FL MGUARD RS4000*, FL MGUARD DELTA TX/TX only

Network >> Interfaces >> General ("Router" network mode, "Modem/Built-in Modem" router mode)	
Modem/Built-in Modem	For all of the devices mentioned above, data traffic is routed via the serial interface and not via the FL MGUARD WAN port when in *Modem* or *Built-in Modem* network mode. From there it is: – Routed via the external serial interface (serial port), to which an external modem must be connected In *Modem* network mode, the serial interface of the FL MGUARD is not available for the PPP dial-in option or for configuration purposes (see "Modem/Console" on page 138). After selecting **Modem** as the network mode, specify the required parameters for the modem connection on the **Dial-out** and/or **Dial-in** tab pages (see "Dial-out" on page 130 and "Dial-in" on page 136). **Enter the connection settings for an external modem on the** *Modem/Console* **tab page (see "Modem/Console" on page 138).** **The configuration of the internal networks is described in the next section.**

5.3.1.2 Ethernet

Network >> Interfaces >> Ethernet		
ARP Timeout	**ARP Timeout**	Service life (in seconds) of entries in the ARP table.
MTU Settings	**MTU of the ... interface**	The maximum transfer unit (MTU) defines the maximum IP packet length that may be used for the relevant interface.
		For a VLAN interface:
		i As VLAN packets contain 4 bytes more than those without VLAN, certain drivers may have problems processing these larger packets. Such problems can be solved by reducing the MTU to 1496.
MAU Configuration		Configuration and status indication of the Ethernet connections:
	Port	Name of the Ethernet connection to which the row refers.
	Media Type	Media type of the Ethernet connection.
	Link State	– Up: The connection is established. – Down: The connection is not established.
	Automatic Configuration	– Yes: Try to determine the required operating mode automatically. – No: Use the operating mode specified in the "Manual Configuration" column.
	Manual Configuration	The desired operating mode when *Automatic Configuration* is set to *No*.
	Current Mode	The current operating mode of the network connection.
	Port On	**Yes/No** Enables/disables the Ethernet connection.

5.3.1.3 Dial-out

i | *FL MGUARD RS4000*, FL MGUARD DELTA TX/TX only.

Network >> Interfaces >> Dial-out		
PPP dial-out options		
This menu item is not included in the scope of functions for the FL MGUARD RS2000.	i	Should only be configured if the FL MGUARD is to be able to establish a data connection (dial-out) to the WAN (Internet):
		– Via the primary external interface (*Modem* or *Built-in Modem* network mode) **or**
		– Via the secondary external interface (also available in *Stealth* or *Router* network mode)

Phone number to call	Phone number of the Internet service provider. The connection to the Internet is established after establishing the telephone connection.
	Command syntax:
	Together with the previously set ATD modem command for dialing, the following dial sequence, for example, is created for the connected modem: ATD765432.
	A compatible pulse dialing procedure that works in all scenarios is used as standard.
	Special dial characters can be used in the dial sequence.

Network >> Interfaces >> Dial-out [...]		
		HAYES special dial characters
		– **W :** Instructs the modem to insert a dialing pause at this point until the dial tone can be heard.
		Used when the modem is connected to a private branch exchange. An external line must be obtained first for outgoing calls by dialing a specific number (e.g., 0) before the phone number of the relevant subscriber can be dialed. Example: ATD0W765432
		– **T** : Switch to tone dialing.
		Insert the special dial character T before the phone number if the faster tone dialing procedure is to be used (with tone-compatible telephone connections). Example: ATDT765432
	Authentication	PAP/CHAP/None
		PAP = Password Authentication Protocol, CHAP = Challenge Handshake Authentication Protocol. These terms describe procedures for the secure transmission of authentication data using the Point-to-Point Protocol.
		If the Internet service provider requires the user to login using a user name and password, then PAP or CHAP is used as the authentication method. The user name, password, and any other data that must be specified by the user to establish a connection to the Internet are given to the user by the Internet service provider.
		The corresponding fields are displayed depending on whether **PAP**, **CHAP** or **None** is selected. Enter the corresponding data in these fields.

If authentication is via PAP:

Authentication	PAP ▼
User name	
Password	
PAP server authentication	No ▼
Dial on demand	Yes ▼
Idle timeout	Yes ▼
Idle time (seconds)	300
Local IP	0.0.0.0
Remote IP	0.0.0.0
Netmask	0.0.0.0

User name	User name specified during Internet service provider login to access the Internet.
Password	Password specified during Internet service provider login to access the Internet.
PAP server authentication	**Yes/No** The following two entry fields are shown when **Yes** is selected:

Network >> Interfaces >> Dial-out [...]

	Server user name	User name and password that the FL MGUARD requests from the server. The FL MGUARD only allows the connection if the server returns the agreed user name/password combination.
	Server password	
	Subsequent fields	See under "If "None" is selected as the authentication method" on page 132.

If authentication is via CHAP:

Authentication	CHAP ▾
Local name	
Remote name	
Secret for client authentication	
CHAP server authentication	No ▾
Dial on demand	Yes ▾
Idle timeout	Yes ▾
Idle time (seconds)	300
Local IP	0.0.0.0
Remote IP	0.0.0.0
Netmask	0.0.0.0

Local name	A name for the FL MGUARD that it uses to log into the Internet service provider. The service provider may have several customers and it uses this name to identify who is attempting to dial in.
	After the FL MGUARD has logged into the Internet service provider with this name, the service provider also compares the password specified for client authentication (see below).
	The connection can only be established successfully if the name is known to the service provider and the password matches.
Remote name	A name assigned to the FL MGUARD by the Internet service provider for identification purposes. The FL MGUARD will not establish a connection to the service provider if the ISP does not assign the correct name.
Secret for client authentication	Password that must be specified during Internet service provider login to access the Internet.
CHAP server authentication	**Yes/No**
	The following two entry fields are shown when **Yes** is selected:
Password for server authentication	Password that the FL MGUARD requests from the server. The FL MGUARD only allows the connection if the server returns the agreed password.
Subsequent fields	See under "If "None" is selected as the authentication method" on page 132.
If "None" is selected as the authentication method	In this case, the fields that relate to the PAP or CHAP authentication methods are hidden.

Network >> Interfaces >> Dial-out [...]

	Only the fields that define further settings remain visible below.

Authentication	None ▼
Dial on demand	Yes ▼
Idle timeout	Yes ▼
Idle time (seconds)	300
Local IP	0.0.0.0
Remote IP	0.0.0.0
Netmask	0.0.0.0

Other common settings

Network >> Interfaces >> Dial-out

PPP dial-out options	Dial on demand	Yes/No
		ℹ Whether *Yes* or *No*: The telephone connection is always established by the FL MGUARD.
		If set to **Yes** (default): This setting is useful for telephone connections where costs are calculated according to the connection time.
		The FL MGUARD only commands the modem to establish a telephone connection when network packets are actually to be transferred. It also instructs the modem to terminate the telephone connection as soon as no more network packets are to be transmitted for a specific time (see value in *Idle timeout* field). By doing this, however, the FL MGUARD is not constantly available externally, i.e., for incoming data packets.

Network >> Interfaces >> Dial-out [...]

> ℹ️ The FL MGUARD also often or sporadically establishes a connection via the modem, or keeps a connection longer, if the following conditions apply:

– Often: The FL MGUARD is configured so that it synchronizes its system time (date and time) regularly with an external NTP server.
– Sporadically: The FL MGUARD acts as a DNS server and must perform a DNS request for a client.
– After a restart: An active VPN connection is set to **initiate**. If this is the case, the FL MGUARD establishes a connection after every restart.
– After a restart: For an active VPN connection, the gateway of the partner is specified as the host name. After a restart, the FL MGUARD must request the IP address that corresponds to the host name from a DNS server.
– Often: VPN connections are set up and DPD messages are sent regularly (see "Dead Peer Detection" on page 249).
– Often: The FL MGUARD is configured to send its external IP address regularly to a DNS service, e.g., DynDNS, so that it can still be accessed via its host name.
– Often: The IP addresses of partner VPN gateways must be requested from the DynDNS service or they must be kept up-to-date by new queries.
– Sporadically: The FL MGUARD is configured so that SNMP traps are sent to the remote server.
– Sporadically: The FL MGUARD is configured to permit and accept remote access via HTTPS, SSH or SNMP. (The FL MGUARD then sends reply packets to every IP address from which an access attempt is made (if the firewall rules permit this access)).
– Often: The FL MGUARD is configured to connect to an HTTPS server at regular intervals in order to download any configuration profiles available there (see "Management >> Central Management" on page 100).

When **No** is selected, the FL MGUARD establishes a telephone connection using the connected modem as soon as possible after a restart or activation of *Modem* network mode. This remains permanently in place, regardless of whether or not data is transmitted. If the telephone connection is then interrupted, the FL MGUARD attempts to restore it immediately. Thus a permanent connection is created, like a permanent line. By doing this, the FL MGUARD is constantly available externally, i.e., for incoming data packets.

Idle timeout	**Yes/No**
	Only considered when *Dial on demand* is set to **Yes**.
	When set to **Yes** (default), the FL MGUARD terminates the telephone connection as soon as no data traffic is transmitted over the time period specified under *Idle time*. The FL MGUARD gives the connected modem the relevant command for terminating the telephone connection.
	When set to **No**, the FL MGUARD does not give the connected modem a command for terminating the telephone connection.

Network >> Interfaces >> Dial-out [...]		
	Idle time (seconds)	Default: 300. If there is still no data traffic after the time specified here has elapsed, the FL MGUARD can terminate the telephone connection (see above under *Idle timeout*).
	Local IP	IP address of the serial interface of the FL MGUARD that now acts as the WAN interface. If this IP address is assigned dynamically by the Internet service provider, use the preset value: 0.0.0.0.
		Otherwise, e.g., for the assignment of a fixed IP address, enter this here.
	Remote IP	IP address of the partner. When connecting to the Internet, this is the IP address of the Internet service provider, which is used to provide access to the Internet. As the Point-to-Point Protocol (PPP) is used for the connection, the IP address does not usually have to be specified. This means you can use the preset value: 0.0.0.0.
	Netmask	The subnet mask specified here belongs to both the *Local IP* address and the *Remote IP* address. Normally all three values (*Local IP, Remote IP, Netmask*) are either fixed or remain set to 0.0.0.0.
		Enter the connection settings for an external modem on the *Modem/Console* tab page (see "Modem/Console" on page 138).

5.3.1.4 Dial-in

> **i** *FL MGUARD RS4000*, FL MGUARD DELTA TX/TX only.

Network >> Interfaces >> Dial-in

PPP dial-in options

This menu item is not included in the scope of functions for the FL MGUARD RS2000.

> **i** *FL MGUARD RS4000*, FL MGUARD DELTA TX/TX only.

Should only be configured if the FL MGUARD is to permit PPP dial-in via one of the following:

– A modem connected to the serial interface
– A built-in modem (available as an option for the FL MGUARD industrial rs).

PPP dial-in can be used to access the LAN (or the FL MGUARD for configuration purposes) (see "Modem/Console" on page 138).

If the modem is used for dialing out by acting as the primary external interface (*Modem* network mode) of the FL MGUARD or as its secondary external interface (when activated in *Stealth* or *Router* network mode), it is not available for the PPP dial-in option.

Modem (PPP)	*FL MGUARD RS4000* **only**.
	Off/On
	This option **must** be set to "Off" if no serial interface is to be used for the PPP dial-in option.
	If this option is set to **On**, the PPP dial-in option is available. The connection settings for the connected external modem should be made on the *Modem/Console* tab page.
Local IP	IP address of the FL MGUARD via which it can be accessed for a PPP connection.
Remote IP	IP address of the partner of the PPP connection.

Network >> Interfaces >> Dial-in [...]		
	PPP Login name	Login name that must be specified by the PPP partner in order to access the FL MGUARD via a PPP connection.
	PPP Password	The password that must be specified by the PPP partner in order to access the FL MGUARD via a PPP connection.
Incoming Rules (PPP)		Firewall rules for PPP connections to the LAN interface.
		If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.
		The following options are available:
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
	From/To Port	(Only evaluated for TCP and UDP protocols.)
		any refers to any port.
		startport:endport (e.g., 110:120) refers to a port area.
		Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	Action	**Accept** means that the data packets may pass through.
		Reject means that the data packets are sent back and the sender is informed of their rejection.
		Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule:
		– Should be logged – set *Log* to **Yes**
		– Should not be logged – set *Log* to **No** (default settings).
	Log entries for unknown connection attempts	Yes/No
		When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged.
	Outgoing Rules (Port)	Firewall rules for outgoing PPP connections from the LAN interface.
		The parameters correspond to those under *Incoming Rules (PPP)*.
		These outgoing rules apply to data packets that are sent out via a data link initiated by PPP dial-in.

5.3.1.5   Modem/Console

ℹ️ *FL MGUARD RS4000/RS2000, FL MGUARD SMART2*, FL MGUARD DELTA TX/TX only.

Some FL MGUARD models have a serial interface that can be accessed externally, while the FLFL MGUARD industrial rs is also available with a built-in modem as an option (see "Network >> Interfaces" on page 104).

Network » Interfaces

General	Ethernet	Dial-out	Dial-in	Modem / Console

Serial Console

Baudrate	57600 ▼
Hardware handshake RTS/CTS	Off ▼

<u>Please note:</u>On some platforms the serial port is not accessible. The settings above become effective only for administrative shell login via a console connected to the serial port. Such logins are impossible if dial-in or dial-out is configured via external modem.

External Modem

Hardware handshake RTS/CTS	Off ▼
Baudrate	57600
Handle modem transparently (for dial-in only)	Yes ▼
Modem init string	~\d+++\dATH OK

Options for using the serial interface

The serial interface can be used alternatively as follows:

Primary external interface (This menu item is not included in the scope of functions for the FL MGUARD RS2000.)

As a **primary external interface**, if the network mode is set to *Modem* under *Network >> Interfaces* on the *General* tab page (see "Network >> Interfaces" on page 104 and "General" on page 105).

In this case, data traffic is not processed via the WAN port (Ethernet interface), but via the serial interface.

Secondary external interface (This menu item is not included in the scope of functions for the FL MGUARD RS2000.)

As a **secondary external interface**, if *Secondary External Interface* is activated and *Modem* is selected under *Network >> Interfaces* on the *General* tab page (see "Network >> Interfaces" on page 104 and "General" on page 105).

In this case, data traffic is processed (permanently or temporarily) via the serial interface.

For dialing in to the LAN or for configuration purposes (This menu item is not included in the scope of functions for the FL MGUARD RS2000.)

Used for **dialing in to the LAN or for configuration purposes** (see also "Dial-in" on page 136). The following options are available:

–   A modem is connected to the serial interface of the FL MGUARD. This modem is connected to the telephone network (fixed-line or GSM network).

(The connection to the telephone network is established via the terminal strip on the bottom of the device for the FL MGUARD RS ... **with** built-in modem or ISDN terminal adapter.)

This enables a remote PC that is also connected to the telephone network to establish a PPP (Point-to Point Protocol) dial-up line connection to the FL MGUARD via a modem or ISDN adapter.

This method is referred to as a PPP dial-in option. It can be used to access the LAN behind the FL MGUARD or to configure the FL MGUARD. *Dial-in* is the interface definition used for this connection type in firewall selection lists.

In order to access the LAN with a Windows computer using the dial-up line connection, a network connection must be set up on this computer in which the dial-up line connection to the FL MGUARD is defined. In addition, the IP address of the FL MGUARD (or its host name) must be defined as the gateway for this connection so that the connections to the LAN can be routed via this address.

To access the web configuration interface of the FL MGUARD, you must enter the IP address of the FL MGUARD (or its host name) in the address line of the web browser.

– The serial interface of the FL MGUARD is connected to the serial interface of a PC.

On the PC, the connection to the FL MGUARD is established using a terminal program and the configuration is implemented using the command line of the FL MGUARD.

If an external modem is connected to the serial interface, you may have to enter corresponding settings below under *External Modem*, regardless of the use of the serial port and the modem connected to it.

Network >> Interfaces >> Modem/Console		
Serial Console		
	ℹ️ The following settings for the *Baudrate* and *Hardware handshake* are only valid for a configuration connection where a terminal or PC with terminal program is connected to the serial interface as described above. The settings are not valid when an external modem is connected. Settings for this are made further down under *External Modem*.	
	Baudrate	The transmission speed of the serial interface is specified via the selection list.
	Hardware handshake RTS/CTS	**Off/On** When set to **On**, flow is controlled by means of RTS and CTS signals.
	Serial console via USB (FL MGUARD SMART2 only)	**No/Yes** When **No** is selected, the FL MGUARD SMART2 uses the USB connection solely as a power supply. When **Yes** is selected, the FL MGUARD SMART2 provides an additional serial interface for the connected computer through the USB interface. The serial interface can be accessed on the computer using a terminal program. The FL MGUARD SMART2 provides a console through the serial interface, which can then be used in the terminal program. Windows requires a special driver. This can be directly downloaded from the FL MGUARD. The relevant link is located on the right-hand side next to the "Serial console via USB" drop-down menu.
External Modem This menu item is not included in the scope of functions for the FL MGUARD RS2000.	**Hardware handshake RTS/CTS**	**Off/On** When set to **On**, flow is controlled by means of RTS and CTS signals for PPP connections.

Network >> Interfaces >> Modem/Console		
	Baudrate	Default: 57600.
		Transmission speed for communication between the FL MGUARD and modem via the serial connecting cable between both devices.
		This value should be set to the highest value supported by the modem. If the value is set lower than the maximum possible speed that the modem can reach on the telephone line, the telephone line will not be used to its full potential.
	Handle modem transparently (for dial-in only)	**Yes/No**
		If the external modem is used for dial-in (see Page 136), **Yes** means that the FL MGUARD does not initialize the modem. The subsequently configured modem initialization sequence is not observed. Thus, either a modem is connected which can answer calls itself (default profile of the modem contains "auto answer") or a null modem cable to a computer can be used instead of the modem, and PPP protocol is used over this.
	Modem init string	Specifies the initialization sequence that the FL MGUARD sends to the connected modem.
		Default: *" \d+++\dATH OK*
		If necessary, consult the modem user manual for the initialization sequence for this modem.
	The initialization sequence is a sequence of character strings expected by the modem and commands that are then sent to the modem so that the modem can establish a connection.	

The preset initialization sequence has the following meaning:

"(two simple quotation marks placed directly after one another)	The empty character string inside the quotation marks means that the FL MGUARD does not initially expect any information from the connected modem, but instead sends the following text directly to the modem.
\d+++\dATH	The FL MGUARD sends this character string to the modem in order to determine whether the modem is ready to accept commands.
OK	Specifies that the FL MGUARD expects the *OK* character string from the modem as a response to *\d+++\dATH*.

> **i** On many modem models it is possible to save modem default settings to the modem itself. However, this option should not be used.
>
> Initialization sequences should be configured externally instead (i.e., on the FL MGUARD). In the event of a modem fault, the modem can then be replaced quickly and smoothly without changing the modem default settings.

> **i** If the external modem is to be used for incoming calls without the modem default settings being entered accordingly, then you have to inform the modem that it should accept incoming calls after it rings.
>
> If using the extended HAYES command set, append the character string " *AT&S0=1 OK*" (a space followed by "*AT&S0=1*", followed by a space, followed by "*OK*") to the initialization sequence.

> ℹ️ Some external modems, depending on their default settings, require a physical connection to the DTR cable of the serial interface in order to operate correctly.
>
> Because the FL MGUARD models do not provide this cable at the external serial interface, the character string " ***AT&D0 OK***" (a space followed by "***AT&D0***", followed by a space, followed by "***OK***") must be appended to the above initialization sequence. According to the extended HAYES command set, this sequence means that the modem does not use the DTR cable.

> ℹ️ If the external modem is to be used for outgoing calls, it is connected to a private branch exchange, and if this private branch exchange does not generate a dial tone after the connection is opened, then the modem must be instructed not to wait for a dial tone before dialing.
>
> In this case, append the character string " ***ATX3 OK***" (a space followed by "***ATX3***", followed by a space, followed by "***OK***") to the initialization sequence.
>
> In order to wait for the dial tone, the control character "***W***" should be inserted in the *Phone number to call* after the digit for dialing an outside line.

5.3.2 Network >> NAT

5.3.2.1 Masquerading
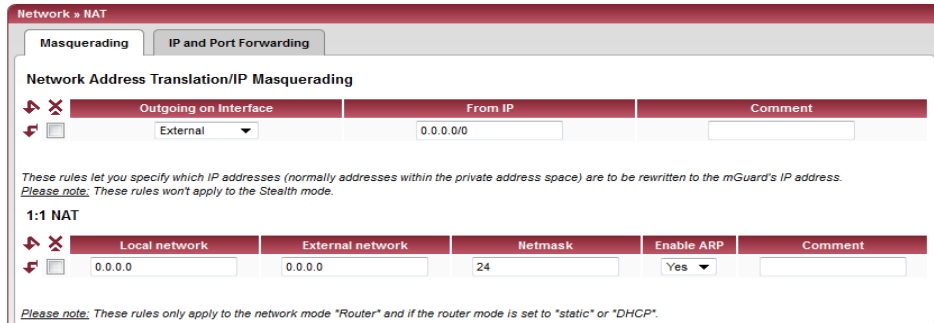
Network >> NAT >> Masquerading	
Network Address Translation/IP Masquerading	Lists the rules established for NAT (**N**etwork **A**ddress **T**ranslation). For outgoing data packets, the device can rewrite the specified sender IP addresses from its internal network to its own external address, a technique referred to as NAT (Network Address Translation), see also NAT (Network Address Translation) in the glossary. This method is used if the internal addresses cannot or should not be routed externally, e.g., because a private address area such as 192.168.x.x or the internal network structure should be hidden. The method can also be used to hide external network structures from the internal devices. To do so, set the **Internal** option under **Outgoing on Interface .** The **Internal** setting allows for communication between two separate IP networks where the IP devices have not configured a (useful) default route or differentiated routing settings (e.g., PLCs without the corresponding settings). The corresponding settings must be made under **1:1 NAT .** This method is also referred to as *IP masquerading*. **Default settings**: NAT is not active. | ⓘ	If the FL MGUARD is operated in *PPPoE/PPTP* mode, NAT must be activated in order to gain access to the Internet. If NAT is not activated, only VPN connections can be used. | | ⓘ	If multiple static IP addresses are used for the WAN port, the first IP address in the list is always used for IP masquerading. | | ⓘ	These rules do not apply in Stealth mode.	
Outgoing on Interface	External/External 2/Any External[1]/Internal Specifies via which interface the data packets are sent so that the rule applies to them. **Any External** refers to the **External** and **External 2** interfaces. A masking is defined, which applies for network data flows in Router mode. These data flows are initiated so that they lead to a destination device which can be accessed over the selected network interface on the FL MGUARD.

Network >> NAT >> Masquerading [...]

		To do this, the FL MGUARD replaces the IP address of the initiator with a suitable IP address of the selected network interface in all associated data packets. The effect is the same as for the other values of the same variables. The IP address of the initiator is hidden from the destination of the data flow. In particular, the destination does not require any routes in order to respond in a data flow of this type (not even a default route (default gateway)).

> ℹ️ Set the firewall in order for the desired connections to be allowed. For incoming and outgoing rules, the source address must still correspond to the original sender if the firewall rules are used.
>
> Please observe the outgoing rules when using the "External/External 2/Any External" settings (see "Outgoing Rules" on page 182).
>
> Please observe the incoming rules when using the "Internal" setting (see "Incoming Rules" on page 180).

From IP	**0.0.0.0/0** means that all internal IP addresses are subject to the NAT procedure. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
Comment	Can be filled with appropriate comments.

1:1 NAT   **Lists the rules established for 1:1 NAT (Network Address Translation).**

With 1:1 NAT, the sender IP addresses are exchanged so that each individual address is exchanged with another specific address, and is not exchanged with the same address for all data packets, as in IP masquerading. This enables the FL MGUARD to mirror addresses from the internal network to the external network.

Example: The FL MGUARD is connected to network 192.168.0.0/24 via its LAN port and to network 10.0.0.0/24 via its WAN port. By using 1:1 NAT, the LAN computer with IP address 192.168.0.8 can be accessed via IP address 10.0.0.8 in the external network.

192.168.0.8   10.0.0.8

192.168.0.0/24   **10.0.0.0/24**

The FL MGUARD claims the IP addresses entered for the "External network" for the devices in its "Local network". The FL MGUARD returns ARP answers for all addresses from the specified "External network" on behalf of the devices in the "Local network". Therefore, the IP addresses entered under "External network" must not be used. They must not be assigned to other devices or used in any way, as an IP address conflict would otherwise occur in the external network. This even applies when no device exists in the "Internal network" for one or more IP addresses from the specified "External network".

Network >> NAT >> Masquerading [...]	
	Default settings: 1:1 NAT is not active.
	ⓘ 1:1 NAT cannot be applied to the *External 2* interface.
	ⓘ 1:1 NAT is only used in *Router* network mode.
	Local network The address of the network on the LAN port.
	External network The address of the network on the WAN port.
	Netmask The subnet mask as a value between 1 and 32 for the local and external network address (see also "CIDR (Classless Inter-Domain Routing)" on page 294).
	Comment Can be filled with appropriate comments.

[1] *External 2* and *Any External* are only for devices with a serial interface: FL MGUARD RS4000 (see "Secondary External Interface" on page 115).

5.3.2.2 IP and Port Forwarding

Network » NAT

Masquerading	IP and Port Forwarding

IP and Port Forwarding

Log ID: fw-portforwarding-*N°*-24dfa31b-3649-14fb-8355-000cbe0600f0

N°	Protocol	From IP	From Port	Incoming on IP	Incoming on Port	Redirect to IP	Redirect to Port	Comment	Log
1	TCP ▼	0.0.0.0/0	any	%extern	http	127.0.0.1	http		No ▼

Network >> NAT >> IP and Port Forwarding

IP and Port Forwarding	Lists the rules defined for port forwarding (DNAT = Destination NAT).
	Port forwarding performs the following: The headers of incoming data packets from the external network, which are addressed to the external IP address (or one of the external IP addresses) of the FL MGUARD and to a specific port of the FL MGUARD, are rewritten in order to forward them to a specific computer in the internal network and to a specific port on this computer. In other words, the IP address and port number in the header of incoming data packets are changed.
	This method is also referred to as Destination NAT.

> **i** Port forwarding cannot be used for connections initiated via the *External 2*[1] interface.

> [1] *External 2* is only for devices with a serial interface.

> **i** The rules defined here have priority over the settings made under Network Security >> Packet Filter >> Incoming Rules .

Protocol: TCP/UDP/GRE	Specify the protocol to which the rule should apply.
	GRE
	GRE protocol IP packets can be forwarded. However, only one GRE connection is supported at any given time. If more than one device sends GRE packets to the same external IP address, the FL MGUARD may not be able to feed back reply packets correctly. We recommend only forwarding GRE packets from specific transmitters. These could be ones that have had a forwarding rule set up for their source address by entering the transmitter address in the "From IP" field, e.g., 193.194.195.196/32.
From IP	The sender address for forwarding.
	0.0.0.0/0 means all addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
From Port	The sender port for forwarding.
	any refers to any port.
	Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80.

Network >> NAT >> IP and Port Forwarding [...]		
	Incoming on IP	– Specify the external IP address (or one of the external IP addresses) of the FL MGUARD here, **or**
		– Use the variable **%extern** (if the external IP address of the FL MGUARD is changed dynamically so that the external IP address cannot be specified).
		If multiple static IP addresses are used for the WAN port, the **%extern** variable always refers to the first IP address in the list.
	Incoming on Port	The original destination port specified in the incoming data packets.
		Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80.
		This information is not relevant for the "GRE" protocol. It is ignored by the FL MGUARD.
	Redirect to IP	The internal IP address to which the data packets should be forwarded and into which the original destination addresses are translated.
	Redirect to Port	The port to which the data packets should be forwarded and into which the original port data is translated.
		Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80.
		This information is not relevant for the "GRE" protocol. It is ignored by the FL MGUARD.
	Comment	Freely selectable comment for this rule.
	Log	For each individual port forwarding rule, you can specify whether the use of the rule:
		– Should be logged – set *Log* to **Yes**
		– Should not be logged – set *Log* to **No** (default settings).

5.3.3 Network >> DNS

5.3.3.1 DNS server
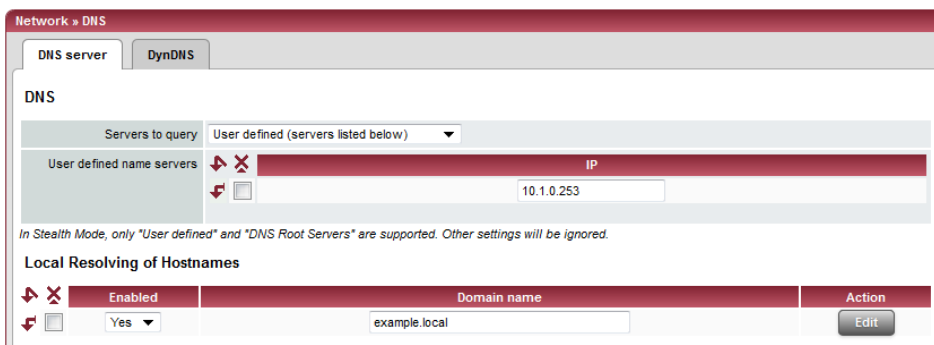
Network >> DNS >> DNS server	
DNS	If the FL MGUARD is to initiate a connection to a partner on its own (e.g., to a VPN gateway or NTP server) and it is specified in the form of a host name (i.e., www.example.com), the FL MGUARD must determine which IP address belongs to the host name. To do this, the FL MGUARD connects to a domain name server (DNS) to query the corresponding IP address there. The IP address determined for the host name is stored in the cache so that it can be found directly (i.e., more quickly) for other host name resolutions.
	With the *Local Resolving of Hostnames* function, the FL MGUARD can also be configured to respond to DNS requests for locally used host names itself by accessing an internal, previously configured directory.
	The locally connected clients can be configured (manually or via DHCP) so that the local address of the FL MGUARD is used as the address of the DNS server to be used. If the FL MGUARD is operated in *Stealth* mode, the management IP address of the FL MGUARD (if this is configured) must be used for the clients, or the IP address 1.1.1.1 must be entered as the local address of the FL MGUARD.
	Servers to query – **DNS Root Servers** Requests are sent to the root name servers on the Internet whose IP addresses are stored on the FL MGUARD. These addresses rarely change. – **Provider defined (e.g., via PPPoE or DHCP)** The domain name servers of the Internet service provider that provide access to the Internet are used. Only select this setting if the FL MGUARD operates in *PPPoE*, *PPTP*, *Modem* mode or in *Router* mode with DHCP. – **User defined (servers listed below)** If this setting is selected, the FL MGUARD will connect to the domain name servers listed under *User defined name servers*.
	User defined name servers The IP addresses of domain name servers can be entered in this list. If these should be used by the FL MGUARD, select the *User defined (servers listed below)* option under **Servers to query**.

Network >> DNS >> DNS server [...]

Local Resolving of Hostnames	You can configure multiple entries with assignment pairs of host names and IP addresses for various domain names.
	You have the option to define, change (edit), and delete assignment pairs of host names and IP addresses. You can also activate or deactivate the resolution of host names for a domain. In addition, you can delete a domain with all its assignment pairs.
	Creating a table with assignment pairs for a domain:
	• Open a new row and click on **Edit** in this row.
	Changing or deleting assignment pairs belonging to a domain:
	• Click on **Edit** in the relevant table row.
	After clicking on **Edit**, the *DNS Records* tab page is displayed:
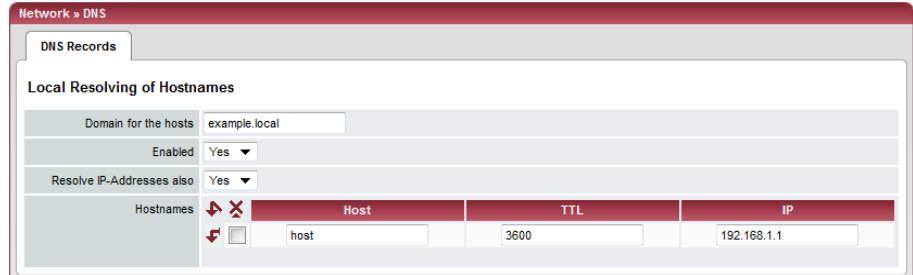
Domain for the hosts	The name can be freely assigned, but it must adhere to the rules for assigning domain names. It is assigned to every host name.
Enabled	**Yes/No**
	Switches the *Local Resolving of Hostnames* function on (**Yes**) or off (**No**) for the domain specified in the field above.
Resolve IP-Addresses also	**No**: The FL MGUARD only resolves host names, i.e., it supplies the assigned IP address for host names.
	Yes: Same as for "No". It is also possible to determine the host names assigned to an IP address.
Hostnames	The table can have any number of entries.
	ℹ️ A host name may be assigned to multiple IP addresses. Multiple host names may be assigned to one IP address.
TTL	Abbreviation for **T**ime **T**o **L**ive. Value specified in seconds. Default: 3600 (= 1 hour)
	Specifies how long called assignment pairs may be stored in the cache of the calling computer.
IP	The IP address assigned to the host name in this table row.
Delete domain with all assignment pairs	Delete the corresponding table entry.

Example: Local Resolving of Hostnames

The "Local Resolving of Hostnames" function is used in the following scenario, for example:

A plant operates a number of identically structured machines, each one as a cell. The local networks of cells A, B, and C are each connected to the plant network via the Internet using the FL MGUARD. Each cell contains multiple control elements, which can be addressed via their IP addresses. Different address areas are used for each cell.

A service technician should be able to use her/his notebook on site to connect to the local network for machine A, B or C and to communicate with the individual controllers. So that the technician does not have to know and enter the IP address for every single controller in machine A, B or C, host names are assigned to the IP addresses of the controllers in accordance with a standardized diagram that the service technician uses. The host names used for machines A, B, and C are identical, i.e., the controller for the packing machine in all three machines has the host name "pack", for example. However, each machine is assigned an individual domain name, e.g., cell-a.example.com.

The service technician can connect her/his notebook to the local network at machine A, B or C and use the same host names in each of these networks to communicate with the corresponding machine controllers.

The notebook can obtain the IP address to be used, the name server, and the domain from the FL MGUARD via DHCP.
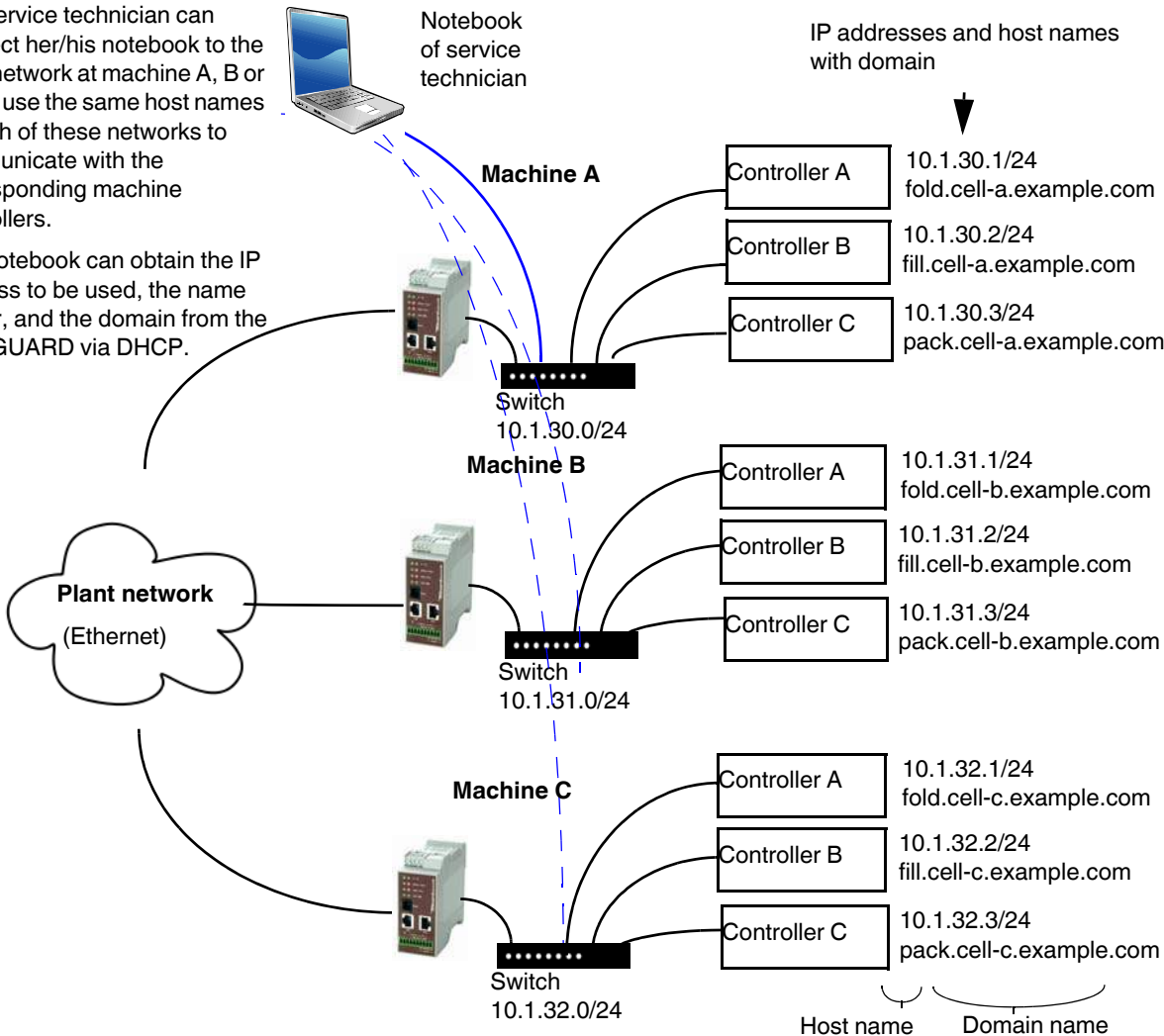
Figure 5-1   Local Resolving of Hostnames

5.3.3.2 DynDNS

Network >> DNS >> DynDNS	
DynDNS	In order for a VPN connection to be established, at least one partner IP address must be known so that the partners can contact each other. This condition is not met if both participants are assigned IP addresses dynamically by their respective Internet service providers. In this case, a DynDNS service such as DynDNS.org or DNS4BIZ.com can be of assistance. With a DynDNS service, the currently valid IP address is registered under a fixed name.
	If you have registered with one of the DynDNS services supported by FL MGUARD, you can enter the corresponding information in this dialog box.
	Register this mGuard at a DynDNS Service? — Select **Yes** if you have registered with a DynDNS provider and if the FL MGUARD is to use this service. The FL MGUARD then reports its current IP address to the DynDNS service (i.e., the one assigned for its Internet connection by the Internet service provider).
	Refresh Interval (sec) — Default: 420 (seconds).
	The FL MGUARD informs the DynDNS service of its new IP address whenever the IP address of its Internet connection is changed. For additional reliability, the device also reports its IP address at the interval specified here.
	This setting has no effect for some DynDNS providers, such as DynDNS.org, as too many updates can cause the account to be closed.
	DynDNS Provider — The providers in this list support the same protocol as the FL MGUARD.
	Select the name of the provider with whom you are registered, e.g., DynDNS.org, TinyDynDNS, DNS4BIZ.
	DynDNS Server — Name of the server for the selected DynDNS provider.
	DynDNS Login, DynDNS Password — Enter the user name and password assigned by the DynDNS provider here.
	DynDNS Hostname — The host name selected for this FL MGUARD at the DynDNS service, providing you use a DynDNS service and have entered the corresponding data above.
	The FL MGUARD can then be accessed via this host name.

5.3.4 Network >> DHCP

The Dynamic Host Configuration Protocol (DHCP) can be used to automatically assign the network configuration set here to the computer connected directly to the FL MGUARD. Under *Internal DHCP* you can specify the DHCP settings for the internal interface (LAN port) and under *External DHCP* the DHCP settings for the external interface (WAN port). The "External DHCP" menu item is not included in the scope of functions for the FL MGUARD RS2000.

> ℹ️ The DHCP server also operates in *Stealth* mode.
>
> In multi stealth mode, the external DHCP server of the FL MGUARD cannot be used if a VLAN ID is assigned as the management IP.

> ℹ️ IP configuration for Windows computers: When you start the DHCP server of the FL MGUARD, you can configure the locally connected computers so that they obtain their IP addresses automatically.

Under Windows XP

- In the Start menu, select "Control Panel, Network Connections".
- Right-click on the LAN adapter icon and select "Properties" from the context menu.
- On the "General" tab, select "Internet Protocol (TCP/IP)" under "This connection uses the following items", then click on "Properties".
- Make the appropriate entries and settings in the "Internet Protocol Properties (TCP/IP)" dialog box.

5.3.4.1 Internal/External DHCP
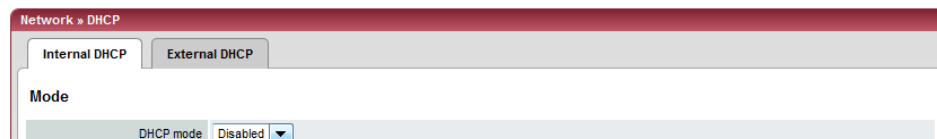
Network >> DHCP >> Internal DHCP		
Mode	**DHCP mode**	**Disabled/Server/Relay**
		Set this option to **Server** if the FL MGUARD is to operate as an independent DHCP server. The corresponding setting options are then displayed below on the tab page (see "Server").
		Set this option to **Relay** if the FL MGUARD is to forward DHCP requests to another DHCP server. The corresponding setting options are then displayed below on the tab page (see "Relay").
		ℹ️ In FL MGUARD *Stealth* mode, *Relay* DHCP mode is not supported. If the FL MGUARD is in *Stealth* mode and *Relay* DHCP mode is selected, this setting will be ignored. However, DHCP requests from the computer and the corresponding responses are forwarded due to the nature of Stealth mode.
		If this option is set to **Disabled**, the FL MGUARD does not answer any DHCP requests.

Network >> DHCP >> Internal DHCP [...]		
	DHCP mode **Server**	
	If DHCP mode is set to *Server*, the corresponding setting options are displayed below as follows.	
DHCP Server Options	**Enable dynamic IP address pool**	Set this option to **Yes** if you want to use the IP address pool specified under *DHCP range start* and *DHCP range end* (see below).
		Set this option to "No" if only static assignments should be made using the MAC addresses (see below).
		With enabled dynamic IP address pool:
		When the DHCP server and the dynamic IP address pool have been activated, you can specify the network parameters to be used by the computer:
		DHCP range start/end
		The start and end of the address area from which the DHCP server of the FL MGUARD should assign IP addresses to locally connected computers.
	DHCP lease time	Time in seconds for which the network configuration assigned to the computer is valid. The client should renew its assigned configuration shortly before this time expires. Otherwise it may be assigned to other computers.
	Local netmask	Specifies the subnet mask of the computers. Default: 255.255.255.0
	Broadcast address	Specifies the broadcast address of the computers.
	Default gateway	Specifies which IP address should be used by the computer as the default gateway. Usually this is the internal IP address of the FL MGUARD.
	DNS server	Address of the server used by the computer to resolve host names in IP addresses via the Domain Name Service (DNS).
		If the DNS service of the FL MGUARD is to be used, enter the internal IP address of the FL MGUARD here.

Network >> DHCP >> Internal DHCP [...]

	WINS server	Address of the server used by the computer to resolve host names in addresses via the Windows Internet Naming Service (WINS).
	Static Mapping [according to MAC address]	To find out the **MAC address** of your computer, proceed as follows:

Windows 95/98/ME:

• Start **winipcfg** in a DOS box.

Windows NT/2000/XP:

• Start **ipconfig /all** in a prompt. The MAC address is displayed as the "Physical Address".

Linux:

• Call **/sbin/ifconfig** or **ip link show** in a shell.

The following options are available:

– MAC address of the client/computer (without spaces or hyphens)
– IP address of client

Client IP Address

The static IP address of the computer to be assigned to the MAC address.

i	Static assignments take priority over the dynamic IP address pool.
i	Static assignments must not overlap with the dynamic IP address pool.
i	Do not use one IP address in multiple static assignments, otherwise multiple MAC addresses will be assigned to this IP address.
i	Only one DHCP server should be used per subnetwork.

DHCP mode   **Relay**

If DHCP mode is set to *Relay*, the corresponding setting options are displayed below as follows.
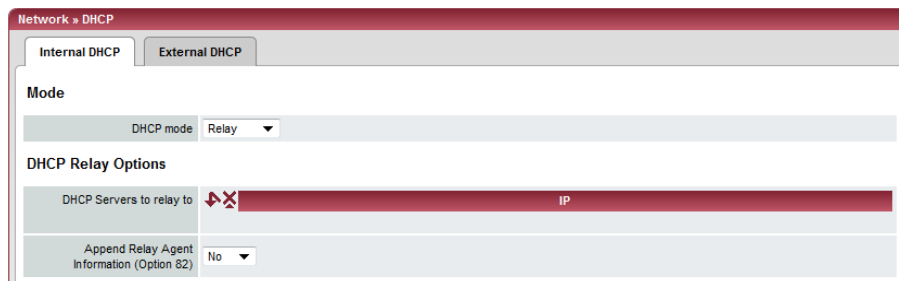
Network >> DHCP >> Internal DHCP [...]

DHCP Relay Options		
	ℹ	In FL MGUARD *Stealth* mode, *Relay* DHCP mode is not supported. If the FL MGUARD is in *Stealth* mode and *Relay* DHCP mode is selected, this setting will be ignored. However, DHCP requests from the computer and the corresponding responses are forwarded due to the nature of Stealth mode.
	DHCP Servers to relay to	A list of one or more DHCP servers to which DHCP requests should be forwarded.
	Append Relay Agent Information (Option 82)	When forwarding, additional information for the DHCP servers to which information is being forwarded can be appended according to RFC 3046.

5.3.5 Network >> Proxy Settings

5.3.5.1 HTTP(S) Proxy Settings

A proxy server can be specified here for the following activities performed by the
FL MGUARD itself:

– CRL download
– Firmware update
– Regular configuration profile retrieval from a central location
– Restoring of licenses

Network >> Proxy Settings >> HTTP(S) Proxy Settings		
HTTP(S) Proxy Settings	Use Proxy for HTTP and HTTPS	When set to **Yes**, connections that use the HTTP or HTTPS protocol are transmitted via a proxy server whose address and port should be specified in the next two fields.
	HTTP(S) Proxy Server	Host name or IP address of the proxy server.
	Port	Number of the port to be used, e.g., 3128.
Proxy Authentication	Login	User name for proxy server login.
	Password	Password for proxy server login.

5.4 Authentication menu

5.4.1 Authentication >> Administrative Users

5.4.1.1 Passwords

Administrative users refers to users who have the right (depending on their authorization level) to configure the FL MGUARD (*root* and *administrator* authorization levels) or to use it (*user* authorization level).

Authentication >> Administrative Users >> Passwords		
	To log into the corresponding authorization level, the user must enter the password assigned to the relevant authorization level (*root*, *admin* or *user*).	
root	**Root Password (Account: root)**	Grants full rights to all parameters of the FL MGUARD.
		Background: Only this authorization level allows unlimited access to the FL MGUARD file system.
		User name (cannot be modified): **root**
		Default root password: **root**
		• To change the root password, enter the old password in the *Old Password* field, then the new password in the two corresponding fields below.
admin	**Administrator Password (Account: admin)**	Grants the rights required for the configuration options accessed via the web-based administrator interface.
		User name (cannot be modified): **admin**
		Default password: **mGuard**

Authentication >> Administrative Users >> Passwords [...]		
user	**Disable VPN until the user is authenticated via HTTP**	If a user password has been specified and activated, the user must always enter this password after an FL MGUARD restart **in order to enable FL MGUARD VPN connections** when attempting to access any HTTP URL.
		To use this option, specify the new user password in the corresponding entry field.
		This option is set to **No** by default.
		If set to **Yes**, VPN connections can only be used once a user has logged into the FL MGUARD via HTTP.
		As long as authentication is required, all HTTP connections are redirected to the FL MGUARD.
		Changes to this option only take effect after the next restart.
	User Password	There is no default user password. To set one, enter the desired password in both entry fields.

5.4.1.2   RADIUS Filters

Group names can be created here for administrative users whose password is checked using a RADIUS server when accessing the FL MGUARD. Each of these groups can be assigned an administrative role.

Authentication >> Administrative Users >> RADIUS Filters	
This menu item is not included in the scope of functions for the FL MGUARD RS2000.	The FL MGUARD only checks passwords using RADIUS servers if you have activated RADIUS authentication:
	– For shell access, see menu: *Management >> System Settings >> Shell Access*
	– For web access, see menu: *Management >> Web Settings >> Access*
	The RADIUS filters are searched consecutively. When the first match is found, access is granted with the corresponding role (*admin*, *netadmin*, *audit*).

Authentication >> Administrative Users >> RADIUS Filters [...]		
	After a RADIUS server has checked and accepted a user's password, it sends the FL MGUARD a list of filter IDs in its response.	
	These filter IDs are assigned to the user in a server database. They are used by the FL MGUARD for assigning the group and hence the authorization level as "admin", "netadmin" or "audit".	
	If authentication is successful, this is noted as part of the FL MGUARD's logging process. Other user actions are logged here using the original name of the user. The log messages are forwarded to a SysLog server, provided a SysLog server has been approved by the FL MGUARD.	
	The following actions are recorded:	
	– Login	
	– Logout	
	– Start of a firmware update	
	– Changes to the configuration	
	– Password changes for one of the predefined users (*root, admin, netadmin, audit, and user*)	
RADIUS Filters for Administrative Access	**Group/Filter ID**	The group name may only be used once. Two lines may not have the same value.
		Answers from the RADIUS server with a notification of successful authentication must have this group name in their filter ID attribute.
		Up to 50 characters are allowed (printable UTF-8 characters only) without spaces.
	Authorized for access as	Each group is assigned an administrative role.
		adminAdministrator
		netadmin: Administrator for the network
		audit: Auditor

5.4.2 Authentication >> Firewall Users

To prevent private surfing on the Internet, for example, every outgoing connection is blocked under *Network Security >> Packet Filter >> Rule Records* . VPN is not affected by this.

Under *Network Security >> User Firewall* , different firewall rules can be defined for certain users, e.g., outgoing connections are permitted. This user firewall rule takes effect as soon as the relevant firewall user(s) (to whom this user firewall rule applies) has (or have) logged in, see "Network Security >> User Firewall" on page 196.

5.4.2.1 Firewall Users

ℹ️ This menu is **not** available on the **FL MGUARD RS2000**.

Administrative access simultaneously via X.509 authentication and via login to the FL MGUARD user firewall is not possible with the **Safari browser**.
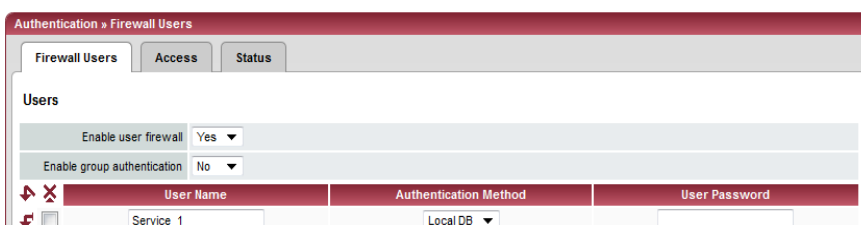
Authentication >> Firewall Users >> Firewall Users		
Users	Lists the firewall users by their assigned user names. Also specifies the authentication method.	
	Enable user firewall	Under the *Network Security >> User Firewall* menu item, firewall rules can be defined and assigned to specific firewall users.
		When set to **Yes**, the firewall rules assigned to the listed users are applied as soon as the corresponding user logs in.
	Enable group authentication	If activated, the FL MGUARD forwards login requests for unknown users to the RADIUS server. If successful, the response from the RADIUS server will contain a group name. The FL MGUARD then enables user firewall templates containing this group name as the template user.
		The RADIUS server must be configured to deliver this group name in the "Access Accept" packet as a "Filter-ID=<groupname>" attribute.
	User Name	Name specified by the user during login.
	Authentication Method	**Local DB**: When *Local DB* is selected, the password assigned to the user must be entered in the *User Password* column in addition to the *User Name* that must be entered on login.
		RADIUS: If RADIUS is selected, the user password can be stored on the RADIUS server.
	User Password	Only active if *Local DB* is selected as the authentication method.

5.4.2.2 Access
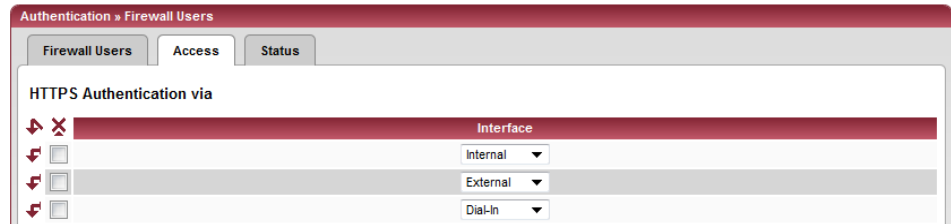
Authentication >> Firewall Users >> Access	
Authentication via HTTPS	ⓘ **NOTE:** For authentication via an external interface, please consider the following:
	If a firewall user can log in via an "unsecure" interface and the user leaves the session without logging out correctly, the login session may remain open and could be misused by another unauthorized person.
	An interface is "unsecure", for example, if a user logs in via the Internet from a location or a computer to which the IP address is assigned dynamically by the Internet service provider – this is usually the case for many Internet users. If such a connection is temporarily interrupted, e.g., because the user logged in is being assigned a different IP address, this user must log in again.
	However, the old login session under the old IP address remains open. This login session could then be used by an intruder, who uses this "old" IP address of the authorized user and accesses the FL MGUARD using this sender address. The same thing could also occur if an (authorized) firewall user forgets to log out at the end of a session.
	This hazard of logging in via an "unsecure interface" is not completely eliminated, but the time is limited by setting the configured timeout for the user firewall template used. See "Timeout type" on page 197
	Interface **External/Internal/External 2/Dial-in[1]**
	Specifies which FL MGUARD interfaces can be used by firewall users to log into the FL MGUARD. For the interface selected, web access via HTTPS must be enabled: **Management**, **Web Settings** menu, *Access* tab page (see "Access" on page 69).
	ⓘ In *Stealth* network mode, both the **Internal** and **External** interfaces must be enabled so that firewall users can log into the FL MGUARD. (Two rows must be entered in the table for this.)

[1] *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 104).

5.4.2.3 Status

When the user firewall is activated, its status is displayed here.

Authentication » Firewall Users
Firewall Users	Access	**Status**

Status

No users are logged in.

5.4.3 Authentication >> RADIUS Servers

Authentication » RADIUS

RADIUS Servers

RADIUS Servers

	RADIUS timeout	3		seconds	
	RADIUS retries	3			

↩ ✗		Server	Via VPN	Port	Secret
↩	☐	radius1.example.com	No ▼	1812	secret
↩	☐	radius2.example.com	Yes ▼	1812	secret
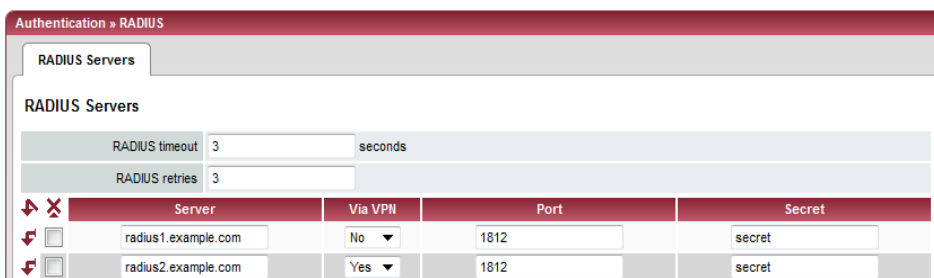
A RADIUS server is a central authentication server used by devices and services for checking user passwords. The password is not known to these devices and services. Only one or a number of RADIUS servers know the password.

The RADIUS server also provides the device or service that a user wishes to access with further information about the user, e.g., the group to which the user belongs. In this way, all user settings can be managed centrally.

In order to activate RADIUS authentication, **Yes** must be set under *Authentication >> Firewall Users (Enable group authentication sub-item) and *RADIUS* selected as the *Authentication Method .*

Under Authentication >> RADIUS Servers, a list of RADIUS servers used by the FL MGUARD is generated. This list is also used when RADIUS authentication is activated for administrative access (SSH/HTTPS).

When RADIUS authentication is active, the login attempt is forwarded from a non-predefined user (not *root*, *admin*, *netadmin*, *audit* or *user*) to all RADIUS servers listed here. The first response received by the FL MGUARD from one of the RADIUS servers determines whether or not the authentication attempt is successful.

Authentication >> RADIUS Servers		
RADIUS Servers This menu item is not included in the scope of functions for the FL MGUARD RS2000.	**RADIUS timeout**	Specifies the time (in seconds) the FL MGUARD waits for a response from the RADIUS server. Default: 3 (seconds).
	RADIUS retries	Specifies how often requests to the RADIUS server are repeated after the RADIUS timeout time has elapsed. Default: 3

Authentication >> RADIUS Servers [...]		
	RADIUS NAS ID	A NAS ID (NAS identifier) is sent with every RADIUS request, except when the field remains empty.
		All common characters on the keyboard (except for umlauts) can be used as the NAS ID.
		The NAS ID is a RADIUS attribute that can be used by the client to be identified by the RADIUS server. The NAS ID can be used instead of an IP address to identify the client. It must be unique within the range of the RADIUS server.
	Server	Name of the RADIUS server or its IP address.
		We recommend entering IP addresses as servers instead of names, where possible. Otherwise, the FL MGUARD must first resolve the names before it can send authentication queries to the RADIUS server. This takes time when logging in. Also, it may not always be possible to perform authentication if name resolution fails (e.g., because the DNS is not available or the name was deleted from the DNS).
	Via VPN	If **Yes** is selected, the FL MGUARD authentication query is always sent via an encrypted VPN tunnel if a suitable one is available.
		If **No** is selected, a query of this type is always sent unencrypted outside the VPN.
	If **Yes** has been selected under **Via VPN** , then the FL MGUARD supports queries from a RADIUS server through its VPN connection. This happens automatically whenever the RADIUS server belongs to the remote network of a configured VPN tunnel and the FL MGUARD has an internal IP address belonging to the local network of the same VPN tunnel. This makes the authentication query dependent on the availability of a VPN tunnel.	
	During configuration, ensure that the failure of a single VPN tunnel does not prevent administrative access to the FL MGUARD.	
	Port	The port number used by the RADIUS server.

Authentication >> RADIUS Servers [...]		
	Secret	RADIUS server password.
		This password must be the same as on the FL MGUARD. The FL MGUARD uses this password to exchange messages with the RADIUS server and to encrypt the user password. The RADIUS server password is not transmitted in the network.
		The password is important for security since the FL MGUARD can be rendered vulnerable to attack at this point if passwords are too weak. We recommend a password with at least 32 characters and several special characters. It must be changed on a regular basis.
		If the RADIUS secret is discovered, an attacker can read the user password for the RADIUS authentication queries. An attacker can also falsify RADIUS responses and gain access to the FL MGUARD if they know the user names. These user names are transmitted as plain text with the RADIUS request. The attacker can thus simulate RADIUS queries and thereby find out user names and the corresponding passwords.
		Administrative access to the FL MGUARD should remain possible while the RADIUS server password is being changed. Proceed as follows to ensure this:
		• Set up the RADIUS server for the FL MGUARD a second time with a new password.
		• Also set this new password on the RADIUS server.
		• On the FL MGUARD, delete the line containing the old password.

5.4.4   Authentication >> Certificates

Authentication is a fundamental element of secure communication. The X.509 authentication method relies on certificates to ensure that the "correct" partners communicate with each other and that no "incorrect" partner is involved in communication. An "incorrect" communication partner is one who falsely identifies themselves as someone they are not, see glossary under "X.509 Certificate".

Certificate   A certificate is used as proof of the identity of the certificate owner. The relevant authorizing body in this case is the CA (certification authority). The digital signature on the certificate is provided by the CA. By providing this signature, the CA confirms that the authorized certificate owner possesses a private key that corresponds to the public key in the certificate.

The name of the certificate issuer appears under *Issuer* on the certificate, while the name of the certificate owner appears under *Subject*.

Self-signed certificates	A self-signed certificate is one that is signed by the certificate owner and not by a CA. In self-signed certificates, the name of the certificate owner appears under both *Issuer* and *Subject*.
	Self-signed certificates are used if communication partners want to or must use the X.509 authentication method without having or using an official certificate. This type of authentication should only be used between communication partners that know and trust each other. Otherwise, from a security point of view, such certificates are as worthless as, for example, a home-made passport without the official stamp.
	Certificates are shown to all communication partners (users or machines) during the connection process, providing the X.509 authentication method is used. In terms of the FL MGUARD, this could apply to the following applications:
	– Authentication of communication partners when establishing VPN connections (see "IPsec VPN >> Connections" on page 222, "Authentication" on page 237).
	– Management of the FL MGUARD via SSH (shell access) (see "Management >> System Settings" on page 50, "Shell Access" on page 58).
	– Management of the FL MGUARD via HTTPS (see "Management >> Web Settings" on page 68, "Access" on page 69).
Certificate, machine certificate	Certificates can be used to identify (authenticate) oneself to others. The certificate used by the FL MGUARD to identify itself to others shall be referred to as the "machine certificate" here, in line with Microsoft Windows terminology.
	A "certificate", "certificate specific to an individual" or "user certificate showing a person" is one used by operators to authenticate themselves to partners (e.g., an operator attempting to access the FL MGUARD via HTTPS and a web browser for the purpose of remote configuration). A certificate specific to an individual can also be saved on a chip card and then inserted by its owner in the card reader of their computer when prompted by a web browser during establishment of the connection, for example.
Remote certificate	A certificate is thus used by its owner (person or machine) as a form of ID in order to verify that they really are the individual they identify themselves as. As there are at least two communication partners, the process takes place alternately: partner A shows their certificate to partner B; partner B then shows their certificate to partner A.
	Provision is made for the following so that A can accept the certificate shown by B, i.e., the certificate of its partner (thus allowing communication with B): A has previously received a copy of the certificate from B (e.g., by data carrier or e-mail) which B will use to identify itself to A. A can then verify that the certificate shown by B actually belongs to B by comparing it with this copy. With regard to the FL MGUARD interface, the certificate copy given here by partner B to A is an example of a *remote certificate*.
	For reciprocal authentication to take place, both partners must thus provide the other with a copy of their certificate in advance in order to identify themselves. A installs the copy of the certificate from B as its remote certificate. B then installs the copy of the certificate from A as its remote certificate.
	Never provide the PKCS#12 file (file name extension: *.p12) as a copy of the certificate to the partner in order to use X.509 authentication for communication at a later time. The PKCS#12 file also contains the private key that must be kept secret and must not be given to a third party (see "Creation of certificates" on page 165).
	To create a copy of a machine certificate imported in the FL MGUARD, proceed as follows:
	• On the "Machine Certificates" tab page, click on **Current Certificate File** next to the *Download Certificate* row for the relevant machine certificate (see "Machine certificates" on page 171).

CA certificates

The certificate shown by a partner can also be checked by the FL MGUARD in a different way, i.e., not by consulting the locally installed remote certificate on the FL MGUARD. To check the authenticity of possible partners in accordance with X.509, the method described below of consulting CA certificates can be used instead or as an additional measure, depending on the application.

CA certificates provide a way of checking whether the certificate shown by the partner is really signed by the CA specified in the partner's certificate.

A CA certificate is available as a file from the relevant CA (file name extension: *.cer, *.pem or *.crt). For example, this file may be available to download from the website of the relevant CA.

The FL MGUARD can then check if the certificate shown by the partner is authentic using the CA certificates loaded on the FL MGUARD. However, this requires all CA certificates to be made available to the FL MGUARD in order to form a chain with the certificate shown by the partner. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the partner to be checked, this also includes the CA certificate of the superordinate CA, and so forth, up to the root certificate (see glossary under CA certificate).

Authentication using CA certificates enables the number of possible partners to be extended without any increased management effort because it is not compulsory to install a remote certificate for each possible partner.

Creation of certificates

To create a certificate, a *private key* and the corresponding *public key* are required. Programs are available so that any user can create these keys. Similarly, a corresponding certificate with the corresponding *public key* can also be created, resulting in a self-signed certificate. (Additional information about self-creation can be downloaded from www.innominate.com. It is available in the download area in an application note entitled "How to obtain X.509 certificates".)

A corresponding certificate signed by a CA must be requested from the CA.

In order for the private key to be imported into the FL MGUARD with the corresponding certificate, these components must be packed into a PKCS#12 file (file name extension: *.p12).

Authentication methods   The FL MGUARD uses two methods of X.509 authentication that are fundamentally different.

– The authentication of a partner is carried out based on the certificate and remote certificate. In this case, the remote certificate that is to be consulted must be specified for each individual connection, e.g., for VPN connections.

– The FL MGUARD consults the CA certificate provided to check whether the certificate shown by the partner is authentic. This requires all CA certificates to be made available to the FL MGUARD in order to form a chain with the certificate shown by the partner through to the root certificate.

"Available" means that the relevant CA certificates must be installed on the FL MGUARD (see "CA certificates" on page 173) and must also be referenced during the configuration of the relevant application (SSH, HTTPS, and VPN).

Whether both methods are used alternatively or in combination varies depending on the application (VPN, SSH, and HTTPS).

Restrictions using the Safari browser

Please note that during administrative access to the FL MGUARD via an X.509 certificate using the **Safari browser** all sub-CA certificates must be installed in the browser's truststore.

Authentication for SSH

The partner shows the following:	Certificate (specific to individual), **signed by CA**	Certificate (specific to individual), **self-signed**
The FL MGUARD authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter[1]	Remote certificate

[1] (See "Management >> System Settings" on page 50, "Shell Access" on page 58)

Authentication for HTTPS

The partner shows the following:	Certificate (specific to individual), **signed by CA**[1]	Certificate (specific to individual), **self-signed**
The FL MGUARD authenticates the partner using:	⇕	⇕
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner PLUS (if required) Remote certificates, **if** used as a filter[2]	Remote certificate

[1] The partner can additionally provide sub-CA certificates. In this case, the FL MGUARD can form the set union for creating the chain from the CA certificates provided and the self-configured CA certificates. The corresponding root CA certificate must always be available on the FL MGUARD.

[2] (See "Management >> Web Settings" on page 68, "Access" on page 69)

Authentication for VPN

The partner shows the following:	Machine certificate, **signed by CA**	Machine certificate, **self-signed**
The FL MGUARD authenticates the partner using:	⇕	⇕
	Remote certificate Or all CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner	Remote certificate

> **NOTE:** It is not sufficient to simply install the certificates to be used on the FL MGUARD under *Authentication >> Certificates* . In addition, the FL MGUARD certificate imported from the pool that is to be used must be referenced in the relevant applications (VPN, SSH, HTTPS).

> The remote certificate for authentication of a VPN connection (or the channels of a VPN connection) is installed in the *IPsec VPN >> Connections* menu.

5.4.4.1 Certificate settings
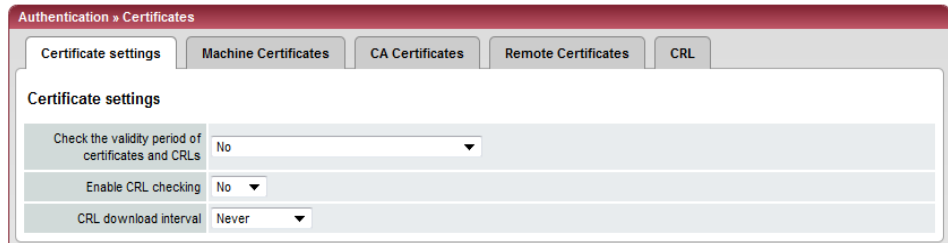
Authentication >> Certificates >> Certificate settings	
Certificate settings	The settings made here relate to all certificates and certificate chains that are to be checked by the FL MGUARD.
	This generally excludes the following:
	– Self-signed certificates from partners
	– All remote certificates for VPN

	Check the validity period of certificates and CRLs	**No**: The validity period specified in certificates and CRLs is ignored by the FL MGUARD.
		Wait for synchronization of the system time
		The validity period specified in certificates and CRLs is only observed by the FL MGUARD if the current date and time are known to the FL MGUARD:
		– By means of the built-in clock (for the *FL MGUARD RS4000/2000, FL MGUARD SMART2*)
		– By synchronizing the system clock (see "Time and Date" on page 53)
		Until this point, all certificates to be checked are considered invalid for security reasons.

Authentication >> Certificates >> Certificate settings [...]		
	Enable CRL checking	**Yes**: When CRL checking is enabled, the FL MGUARD consults the CRL (certificate revocation list) and checks whether or not the certificates that are available to the FL MGUARD are blocked.
		CRLs are issued by the CAs and contain the serial numbers of blocked certificates, e.g., certificates that have been reported stolen.
		On the **CRL** tab page (see "CRL" on page 177), specify the origin of the FL MGUARD revocation lists.
		When CRL checking is enabled, a CRL must be configured for each *issuer* of certificates on the FL MGUARD. Missing CRLs result in certificates being considered invalid.
		Revocation lists are verified by the FL MGUARD using an appropriate CA certificate. Therefore, all CA certificates that belong to a revocation list (all sub-CA certificates and the root certificate) must be imported on the FL MGUARD. If the validity of a revocation list cannot be proven, it is ignored by the FL MGUARD.
		If the use of revocation lists is activated together with the consideration of validity periods, revocation lists are ignored if (based on the system time) their validity has expired or has not yet started.
	CRL download interval	If *Enable CRL checking* is set to **Yes** (see above), select the time period after which the revocation lists should be downloaded and applied.
		On the **CRL** tab page (see "CRL" on page 177), specify the origin of the FL MGUARD revocation lists.
		If CRL checking is enabled, but CRL download is set to **Never**, the CRL must be manually loaded on the FL MGUARD so that CRL checking can be performed.

5.4.4.2 Machine certificates

The FL MGUARD authenticates itself to the partner using a machine certificate loaded on the FL MGUARD. The machine certificate acts as an ID card for the FL MGUARD, which it shows to the relevant partner.

For a more detailed explanation, see "Authentication >> Certificates" on page 163.

By importing a PKCS#12 file, the FL MGUARD is provided with a private key and the corresponding machine certificate. Multiple PKCS#12 files can be loaded on the FL MGUARD, enabling the FL MGUARD to show the desired self-signed or CA-signed machine certificate to the partner for various connections.

In order to use the machine certificate installed at this point, it must be referenced **additionally** during the configuration of applications (SSH, VPN) so that it can be used for the relevant connection or remote access type.

Example of imported machine certificates:
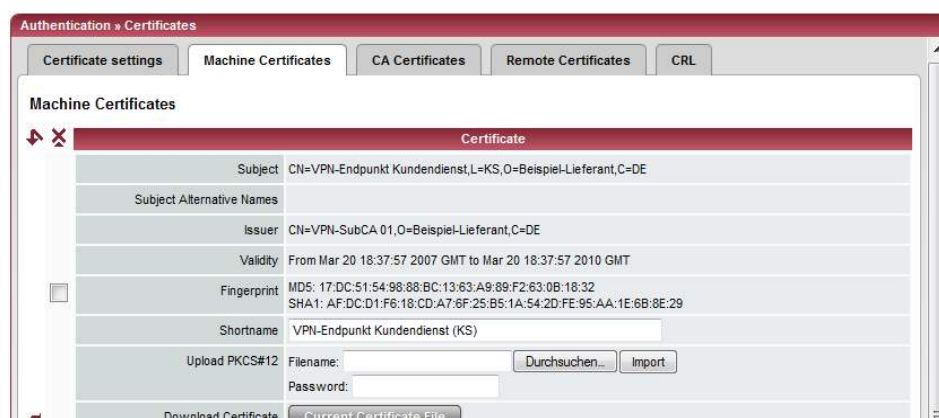
Authentication >> Certificates >> Machine Certificates	
Machine Certificates	**Shows the currently imported X.509 certificates that the FL MGUARD uses to authenticate itself to partners, e.g., other VPN gateways.**

To import a (new) certificate, proceed as follows:

Importing a new machine certificate

Requirement

The PKCS#12 file (file name extension: *.p12 or *.pfx) is saved on the connected computer.

Proceed as follows:
- Click on **Browse...** to select the file.
- In the *Password* field, enter the password used to protect the private key of the PKCS#12 file.
- Click on **Import**.
  Once imported, the loaded certificate appears under *Certificate*.
- Remember to save the imported certificate along with the other entries by clicking on the **Apply** button.

Short name

When importing a machine certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the *Shortname* field is empty at this point). This name can be adopted or another name can be chosen.
- A name must be assigned, whether it is the suggested one or another. Names must be unique and must not be assigned more than once.

Using the short name

During the configuration of
– SSH (*Management >> System Settings , Shell Access* menu)
– HTTPS (*Management >> Web Settings , Access* menu)
– VPN connections (*IPsec VPN >> Connections* menu)

the certificates imported on the FL MGUARD are provided in a selection list.

The certificates are displayed under the short name specified for each individual certificate on this page.

For this reason, name assignment is mandatory.

Creating a certificate copy

You can create a copy of the imported machine certificate (e.g., for the partner in order to authenticate the FL MGUARD). This copy does not contain the private key and can therefore be made public at any time.

To do this, proceed as follows:
- Click on **Current Certificate File** next to the *Download Certificate* row for the relevant machine certificate.
- Enter the desired information in the dialog box that opens.

5.4.4.3 CA certificates

CA certificates are certificates issued by a certification authority (CA). CA certificates are used to check whether the certificates shown by partners are authentic.

The checking process is as follows: The certificate issuer (CA) is specified as the issuer in the certificate transmitted by the partner. These details can be verified by the same issuer using the local CA certificate. For a more detailed explanation, see "Authentication >> Certificates" on page 163.

Example of imported CA certificates:

Authentication » Certificates				
Certificate settings	Machine Certificates	CA Certificates	Remote Certificates	CRL

Trusted CA Certificates

	Certificates
Subject	CN=VPN-RootCA 01,O=Beispiel-Lieferant,C=DE
Subject Alternative Names	
Issuer	CN=VPN-RootCA 01,O=Beispiel-Lieferant,C=DE
Validity	From Mar 20 15:56:38 2007 GMT to Mar 20 15:56:38 2022 GMT
Fingerprint	MD5: 49:13:FB:16:C8:3A:DE:C3:F7:70:AB:F9:5B:76:BD:40 SHA1: 12:C2:4C:53:7B:60:62:FA:C0:83:61:C4:92:98:03:82:75:1D:29:75
Shortname	VPN-RootCA 01
Upload Certificate	Filename: [ ] [Durchsuchen...] [Import]
Download Certificate	[Current Certificate File]

Authentication >> Certificates >> CA Certificates	
Trusted CA Certificates	**Displays the current imported CA certificates.**
	To import a (new) certificate, proceed as follows:
Importing a CA certificate	**Requirement** The file (file name extension: *.cer, *.pem or *.crt) is saved on the connected computer. Proceed as follows: • Click on **Browse...** to select the file. • Click on **Import**. Once imported, the loaded certificate appears under *Certificate*. • Remember to save the imported certificate along with the other entries by clicking on the **Apply** button. **Short name** When importing a CA certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the Shortname field is empty at this point). This name can be adopted or another name can be chosen. • A name must be assigned, whether it is the suggested one or another. Names must be unique and must not be assigned more than once.
Using the short name	During the configuration of – SSH (*Management >> System Settings , Shell Access* menu) – HTTPS (*Management >> Web Settings , Access* menu) – VPN connections (*IPsec VPN >> Connections* menu)

the certificates imported on the FL MGUARD are provided in a selection list. The certificates are displayed under the short name specified for each individual certificate on this page. For this reason, name assignment is mandatory.

Creating a certificate copy

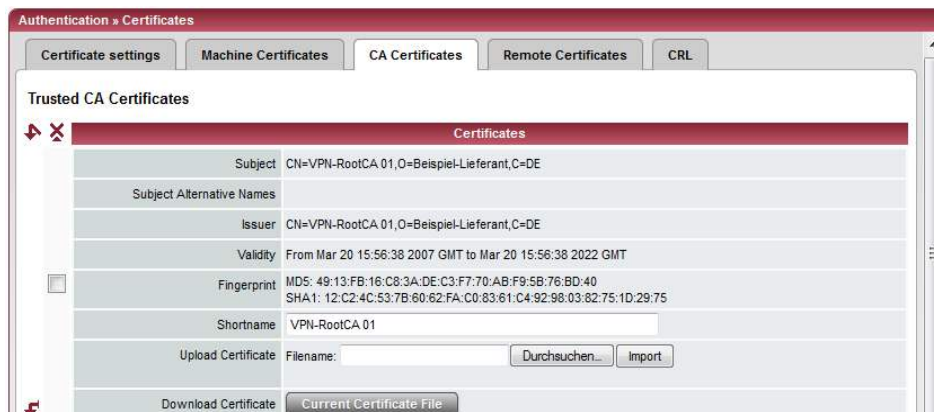A copy can be created from the imported CA certificate.

To do this, proceed as follows:

- Click on **Current Certificate File** next to the *Download Certificate* row for the relevant CA certificate. Enter the desired information in the dialog box that opens.

5.4.4.4   Remote certificates

A remote certificate is a copy of the certificate that is used by a partner to authenticate itself to the FL MGUARD.

Remote certificates are files (file name extension: *.cer, *.pem or *.crt) received from possible partners by trustworthy means. You load these files on the FL MGUARD so that reciprocal authentication can take place. The remote certificates of several possible partners can be loaded.

The remote certificate for authentication of a VPN connection (or the channels of a VPN connection) is installed in the *IPsec VPN >> Connections* menu.

For a more detailed explanation, see "Authentication >> Certificates" on page 163.

Example of imported remote certificates:
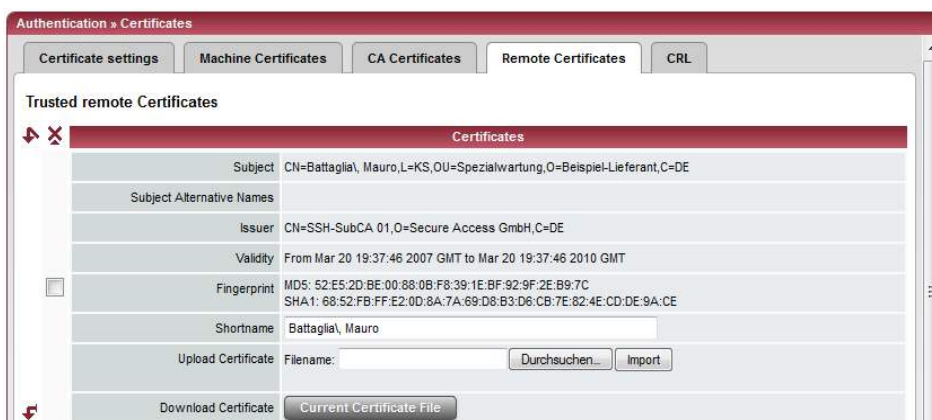
Authentication >> Certificates >> Remote Certificates

Trusted remote Certificates	Displays the current imported remote certificates.
Importing a new certificate	**Requirement** The file (file name extension: *.cer, *.pem or *.crt) is saved on the connected computer. Proceed as follows: • Click on **Browse...** to select the file. • Click on **Import**. Once imported, the loaded certificate appears under *Certificate*. • Remember to save the imported certificate along with the other entries by clicking on the **Apply** button. **Short name** When importing a remote certificate, the CN attribute from the certificate subject field is suggested as the short name here (providing the *Shortname* field is empty at this point). This name can be adopted or another name can be chosen. • A name must be assigned, whether it is the suggested one or another. Names must be unique and must not be assigned more than once.

Using the short name

During the configuration of
– SSH (*Management >> System Settings , Shell Access* menu)
– HTTPS (*Management >> Web Settings , Access* menu)

the certificates imported on the FL MGUARD are provided in a selection list. The certificates are displayed under the short name specified for each individual certificate on this page.

For this reason, name assignment is mandatory.

Creating a certificate copy

A copy can be created from the imported remote certificate.

To do this, proceed as follows:

• Click on **Current Certificate File** next to the *Download Certificate* row for the relevant remote certificate. Enter the desired information in the dialog box that opens.

5.4.4.5 CRL
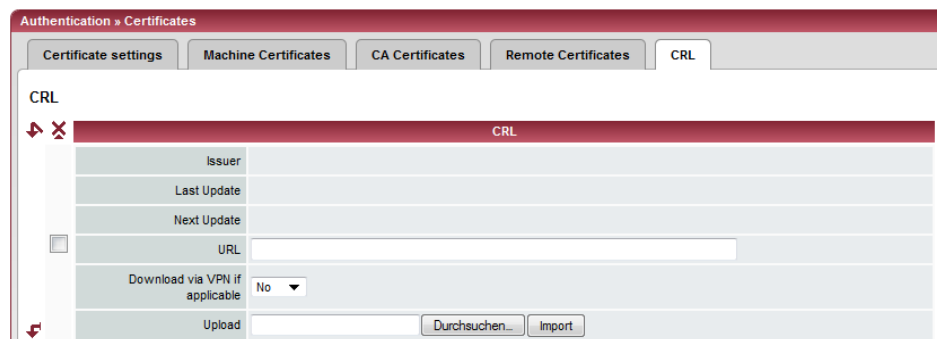
Authentication >> Certificates >> CRL	
CRL	CRL stands for certificate revocation list.
	The CRL is a list containing serial numbers of blocked certificates. This page is used for the configuration of sites from which the FL MGUARD should download CRLs in order to use them.
	Certificates are only checked for revocations if the **Enable CRL checking** option is set to **Yes** (see "Certificate settings" on page 169).
	A CRL with the same issuer name must be present for each issuer name specified in the certificates to be checked. If a CRL is not present and CRL checking is enabled, the certificate is considered invalid.
	Issuer Information read directly from the CRL by the FL MGUARD.
	Shows the issuer of the relevant CRL.
	Last Update Information read directly from the CRL by the FL MGUARD.
	Time and date of issue of the current CRL on the FL MGUARD.
	Next Update Information read directly from the CRL by the FL MGUARD.
	Time and date when the CA will next issue a new CRL.
	This information is not influenced or considered by the CRL download interval.
	URL Specify the URL of the CA where CRL downloads are obtained if the CRL should be downloaded on a regular basis, as defined under **CRL download interval** on the *Certificate settings* tab page (see "Certificate settings" on page 169).
	Download via VPN if applicable If set to **Yes**, the FL MGUARD uses a VPN tunnel to access the URL that the CRL makes available for download. For this to happen, a suitable VPN tunnel must be configured, activated, and allow access. Otherwise, the CRL downloads from this URL will not be forwarded via a VPN tunnel.

Authentication >> Certificates >> CRL		
	Upload	If the CRL is available as a file, it can also be loaded on the FL MGUARD manually. • To do this, click on **Browse...**, select the file, and click on **Import**. • Remember to save the imported CRL along with the other entries by clicking on the "Apply" button. ℹ An up-to-date CRL file must always be used. For this reason, it is not included in the FL MGUARD configuration. When exporting an FL MGUARD configuration and then importing it to another FL MGUARD, the CRL file must be uploaded again. CRL files might be deleted during a firmware update. In this case, the FL MGUARD downloads the CRL files from the specified URL again. Alternatively, it can be uploaded manually.

5.5 Network Security menu

| i | A reduced version of the menu is available on the **FL MGUARD RS2000**. |

5.5.1 Network Security >> Packet Filter

The FL MGUARD includes a *Stateful Packet Inspection Firewall*. The connection data of an active connection is recorded in a database (connection tracking). Rules can thus only be defined for one direction. This means that data from the other direction of the relevant connection, and only this data, is automatically allowed through.

A side effect is that existing connections are not aborted during reconfiguration, even if a corresponding new connection can no longer be established.

Default firewall settings:
– All incoming connections are rejected (excluding VPN).
– Data packets of all outgoing connections are allowed through.

The firewall rules here have an effect on the firewall that is permanently active, with the exception of:
– **VPN connections**. Individual firewall rules are defined for VPN connections (see "IPsec VPN >> Connections" on page 222, "Firewall" on page 243).
– **User firewall**. When a user for whom user firewall rules are defined logs in, these rules take priority (see "Network Security >> User Firewall" on page 196), followed by the permanently active firewall rules.

| i | If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied.
If the list of rules contains further subsequent rules that could also apply, these rules are ignored. |

5.5.1.1 Incoming Rules
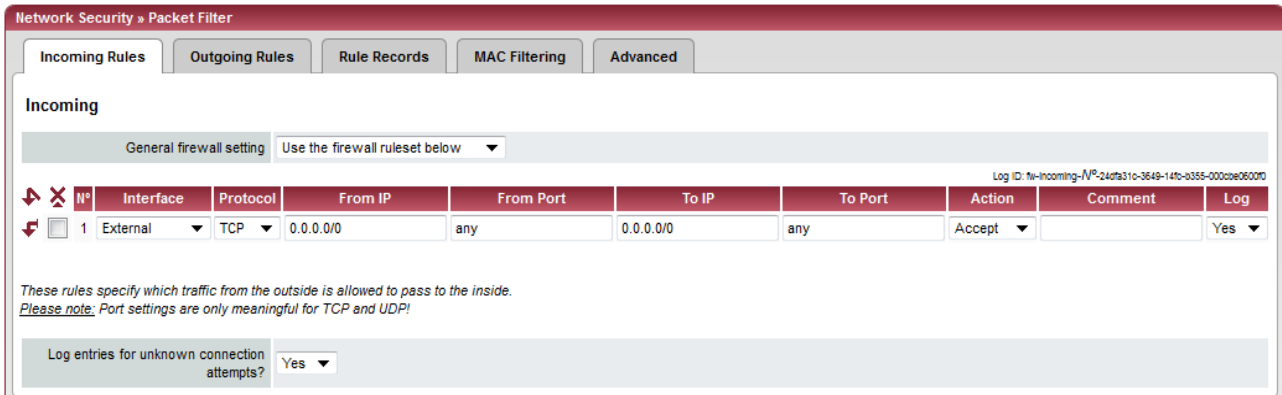
Network Security >> Packet Filter >> Incoming Rules	
Incoming	Lists the firewall rules that have been set up. They apply for incoming data links that have been initiated externally.
	If no rule has been set, the data packets of all incoming connections (excluding VPN) are dropped (default settings).

General firewall setting	**Allow all incoming connections**: The data packets of all incoming connections are allowed.
	Drop all incoming connections: The data packets of all incoming connections are discarded.
	Use the firewall ruleset below: Displays further setting options. (This menu item is not included in the scope of functions for the FL MGUARD RS2000).

The following settings are only visible if "**Use the firewall ruleset below**" is set.

Interface	External/External 2/Any External[1]
	Specifies via which interface the data packets are received so that the rule applies to them. **Any External** refers to the **External** and **External 2** interfaces. These interfaces are only available on FL MGUARD models that have a serial interface with external access.
Protocol	TCP, UDP, ICMP, GRE, All
From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
From Port/To Port	(Only evaluated for TCP and UDP protocols.) – **any** refers to any port. – **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).

Network Security >> Packet Filter >> Incoming Rules [...]		
	Action	**Accept** means that the data packets may pass through.
		Reject means that the data packets are sent back and the sender is informed of their rejection. .
		ⓘ In Stealth mode, **Reject** has the same effect as **Drop**.
		Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
		Name of rule sets, if defined. When a name is specified for rule sets, the firewall rules saved under this name take effect (see *Rule Records* tab page).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule:
		– Should be logged – set *Log* to **Yes**
		– Should not be logged – set *Log* to **No** (default settings).
	Log entries for unknown connection attempts	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged. (Default settings: **No**)

1   *External 2* and *Any External* are only for devices with a serial interface (see "Network >> Interfaces" on page 104).

5.5.1.2 Outgoing Rules
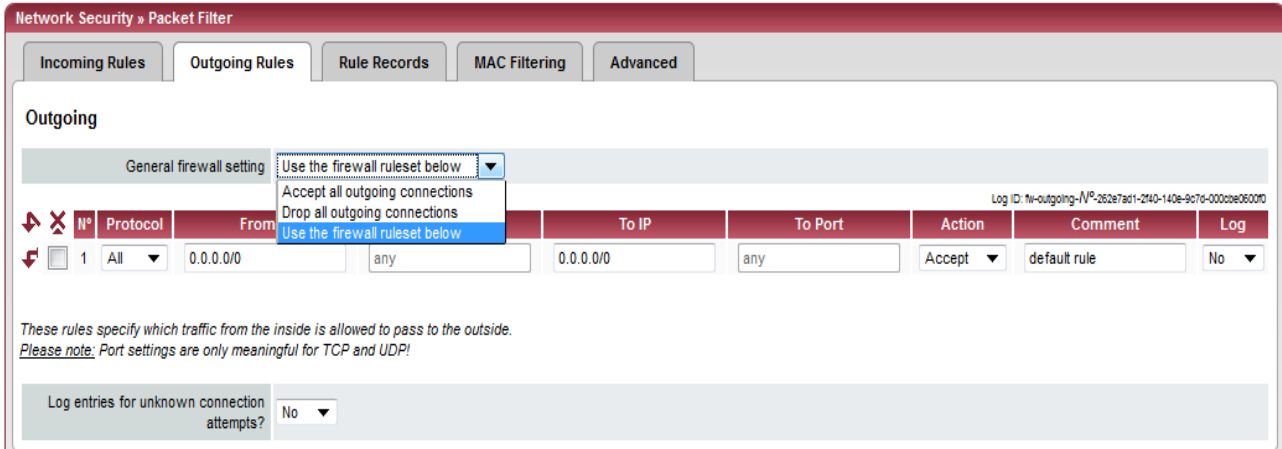
Network Security >> Packet Filter >> Outgoing Rules	
Outgoing	Lists the firewall rules that have been set up. They apply for outgoing data links that have been initiated internally in order to communicate with a remote partner.
	Default setting: A rule is defined by default that allows all outgoing connections.
	If no rule is defined, all outgoing connections are prohibited (excluding VPN).

	General firewall setting	**Allow all outgoing connections**: The data packets of all outgoing connections are allowed.
		Drop all outgoing connections: The data packets of all outgoing connections are discarded.
		Use the firewall ruleset below: Displays further setting options. (This menu item is not included in the scope of functions for the FL MGUARD RS2000).

The following settings are only visible if "**Use the firewall ruleset below**" is set.

|	**Protocol**	TCP, UDP, ICMP, GRE, All
	From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
	From Port/To Port	(Only evaluated for TCP and UDP protocols.) – **any** refers to any port. – **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).

Network Security >> Packet Filter >> Outgoing Rules [...]		
	Action	**Accept** means that the data packets may pass through.
		Reject means that the data packets are sent back and the sender is informed of their rejection. .
		In Stealth mode, **Reject** has the same effect as **Drop**.
		Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
		Name of rule sets, if defined. When a name is specified for rule sets, the firewall rules saved under this name take effect (see *Rule Records* tab page).
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule:
		– Should be logged – set *Log* to **Yes**
		– Should not be logged – set *Log* to **No** (default settings).
	Log entries for unknown connection attempts	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged. (Default settings: **No**)

5.5.1.3 Rule Records

Sets of rules can be defined and stored under a rule set name for structuring incoming and outgoing rules. A rule set can then be referenced in an incoming or outgoing rule, whereby the rules contained in the rule set are applied there.

When defining a rule set, it is also possible to reference another defined rule set, i.e., using this rule set as a block in the current rule set.

Defining a new rule set

- In the set of rules table, click on **Edit** to the right of the "(unnamed)" entry under "Name".
- If the "(unnamed)" entry cannot be seen, open another row in the table.

Editing a rule set

- Click on **Edit** to the right of the relevant entry.
- If a firewall rule set consists of multiple firewall rules, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

Network Security >> Packet Filter >> Rule Records		
Rule Records	**Lists all the defined firewall records of rules.**	
	Records of rules are only used if they are referenced on the *Incoming Rules* or *Outgoing Rules* tab page. A record of rules that is referenced in a firewall rule is only used if it meets all the criteria of this firewall rule.	
	Enabled	Activates/deactivates the relevant set of rules.
	Name	Name of the set of rules. The name is specified when the set of rules is created.

The *Rule Record* page is displayed when you click on **Edit**:
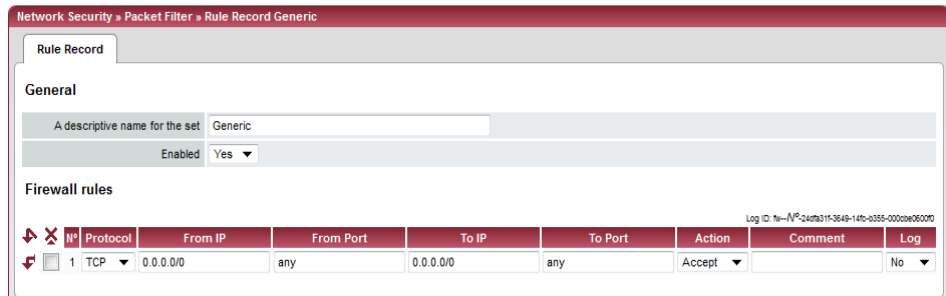
General		
	A descriptive name for the set	A name that can be freely assigned. Although it can be freely selected, the name must clearly define the set of rules. A set of rules can be referenced from the list of incoming and outgoing rules using this name. To do this, the relevant rule set name is selected in the *Action* column.
	Enabled	Activates/deactivates the relevant set of rules.

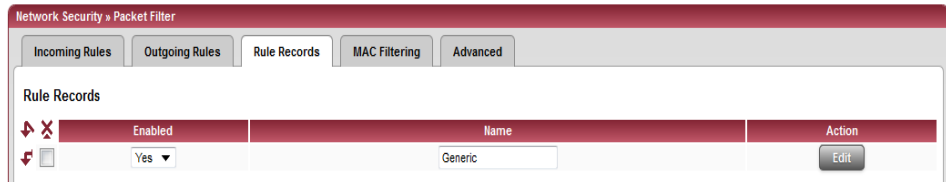| Network Security >> Packet Filter >> Rule Records [...]		
Firewall rules	**Protocol**	TCP, UDP, ICMP, GRE, All
	From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
	From Port/To Port	(Only evaluated for TCP and UDP protocols.) – **any** refers to any port. – **startport:endport** (e.g., 110:120) refers to a port area. Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back and the sender is informed of their rejection. > **i** In Stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts. **Name of rule sets**, if defined. In addition to "Accept", "Reject", and "Drop", the selection list also contains the names of previously defined sets of rules. If a name is selected (referenced), the rules contained in this set of rules are applied here. If the rules from the applied set of rules cannot be used and implemented with "Accept", "Reject" or "Drop", rule processing continues with the rule following the one from which the set of rules was referenced.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).

5.5.1.4 MAC Filtering

The "Incoming" MAC filter is applied to frames that the FL MGUARD receives at the WAN interface. The "Outgoing" MAC filter is applied to frames that the FL MGUARD receives at the LAN interface. Data packets that are received or sent via a modem connection on FL MGUARD models with a serial interface[1] are not picked up by the MAC filter because the Ethernet protocol is not used here.

In *Stealth* mode, in addition to the packet filter (Layer 3/4) that filters data traffic, e.g., according to ICMP messages or TCP/UDP connections, a MAC filter (Layer 2) can also be set. A MAC filter (Layer 2) filters according to MAC addresses and Ethernet protocols.

In contrast to the packet filter, the MAC filter is stateless. This means that if rules are introduced, corresponding rules must also be created for the opposite direction where necessary.

If no rules are set, all ARP and IP packets are allowed to pass through.

> When setting MAC filter rules, please note the information displayed on the screen.
>
> The rules defined here have priority over packet filter rules.
>
> The MAC filter does not support logging.

Network Security >> Packet Filter >> MAC Filtering		
Incoming	**Source MAC**	Specification of the source MAC address: xx:xx:xx:xx:xx:xx stands for all MAC addresses.
	Destination MAC	Specification of the destination MAC address: xx:xx:xx:xx:xx:xx stands for all MAC addresses. ff:ff:ff:ff:ff:ff stands for the broadcast MAC address to which all ARP requests, for example, are sent.

---

1   FL MGUARD RS4000

Network Security >> Packet Filter >> MAC Filtering [...]

	Ethernet Protocol	**%any** stands for all Ethernet protocols.
		Additional protocols can be specified in name or hexadecimal format, for example:
		– IPv4 or 0800
		– ARP or 0806
	Action	**Accept** means that the data packets may pass through.
		Drop means that the data packets are not permitted to pass through (they are dropped).
	Comment	Freely selectable comment for this rule.
Outgoing	The explanation provided under "Incoming" also applies to "Outgoing".	

5.5.1.5 Advanced

The following settings affect the basic behavior of the firewall.

Network Security >> Packet Filter >> Advanced		
Consistency checks This menu item is not included in the scope of functions for the FL MGUARD RS2000.	**Maximum size of "ping" packets (ICMP Echo Request)**	Refers to the length of the entire packet including the header. The packet length is normally 64 bytes, but it can be larger. If oversized packets are to be blocked (to prevent bottlenecks), a maximum value can be specified. This value should be more than 64 bytes in order not to block normal ICMP echo requests.
	Enable TCP/UDP/ICMP consistency checks	When set to **Yes**, the FL MGUARD performs a range of tests to check for incorrect checksums, packet sizes, etc. and drops packets that fail these tests. This option is set to **Yes** by default.

Network Security >> Packet Filter >> Advanced [...]		
	Allow TCP keepalive packets without TCP flags	TCP packets without flags set in their TCP header are normally rejected by firewalls. At least one type of Siemens controller with older firmware sends TCP keepalive packets without TCP flags set. These are therefore discarded as invalid by the FL MGUARD.
		When set to **Yes**, forwarding of TCP packets where no TCP flags are set in the header is enabled. This only applies when TCP packets of this type are sent within an existing TCP connection with a regular structure.
		TCP packets without TCP flags do not result in a new entry in the connection table (see "Connection Tracking" on page 190). If the connection is already established when the FL MGUARD is restarted, the corresponding packets are still rejected and connection problems can be observed as long as no packets with flags belonging to the connection are sent.
		These settings affect all the TCP packets without flags. The **Yes** option thus weakens the security functions provided by the FL MGUARD.
Network Modes (Router/PPTP/PPPoE)	**ICMP via primary external interface for the mGuard**	This option can be used to control the behavior of the FL MGUARD when ICMP messages are received from the external network via the primary/secondary external interface.
	ICMP via secondary external interface for the mGuard	ⓘ Regardless of the setting specified here, incoming ICMP packets are always accepted if SNMP access is activated.
		Drop: All ICMP messages to the FL MGUARD are dropped.
		Allow ping requests: Only ping messages (ICMP type 8) to the FL MGUARD are accepted.
		Allow all ICMPs: All ICMP message types to the FL MGUARD are accepted.
Stealth Mode	**Allow forwarding of GVRP frames**	**Yes/No**
		The GARP VLAN Registration Protocol (GVRP) is used by GVRP-capable switches to exchange configuration information.
		If this option is set to **Yes**, GVRP packets are allowed to pass through the FL MGUARD in *Stealth* mode.
	Allow forwarding of STP frames	**Yes/No**
		The Spanning Tree Protocol (STP) (802.1d) is used by bridges and switches to detect and consider loops in the cabling.
		If this option is set to **Yes**, STP packets are allowed to pass through the FL MGUARD in *Stealth* mode.

Network Security >> Packet Filter >> Advanced [...]		
	Allow forwarding of DHCP frames	**Yes/No**
		When set to **Yes**, the client is allowed to obtain an IP address via DHCP - regardless of the firewall rules for outgoing data traffic.
		This option is set to **Yes** by default.
Connection Tracking	**Maximum table size**	This entry specifies an upper limit. This is set to a level that can never be reached during normal practical operation. However, it can be easily reached in the event of attacks, thus providing additional protection. If there are special requirements in your operating environment, this value can be increased.
		Connections established from the FL MGUARD are also counted. This value must therefore not be set too low, as this will otherwise cause malfunctions.
	Allow TCP connections upon SYN only	**Yes/No, default: No**
		SYN is a special data packet used in TCP/IP connection establishment that marks the beginning of the connection establishment process.
		No (default): The FL MGUARD also allows connections where the beginning has not been registered. This means that the FL MGUARD can perform a restart when a connection is present without interrupting the connection.
		Yes: The FL MGUARD must have registered the SYN packet of an existing connection. Otherwise, the connection is aborted.
		If the FL MGUARD performs a restart while a connection is present, this connection is interrupted. Attacks on and the hijacking of existing connections are thus prevented.
	Timeout for established TCP connections	If a TCP connection is not used during the time period specified here, the connection data is deleted.
		A connection translated by NAT (not 1:1 NAT) must then be reestablished.
		If **Yes** is set under "Allow TCP connections upon SYN only" , all expired connections must be reestablished.
		The default setting is 432000 seconds (5 days).
	Timeout for closed TCP connections	The timeout blocks a TCP port-to-port connection for an extended period after the connection is closed. This is necessary as packets belonging to the closed TCP connection may still arrive in a packet-based network after the connection is closed. Without time-controlled blocking, old packets could be assigned to a new connection accidentally.
		The default setting is 3600 seconds (1 hour).

Network Security >> Packet Filter >> Advanced [...]		
	Reset existing connection after changes to firewall	**Yes/No, default: Yes**
		When set to **Yes**, the existing connections are reset, if the following applies:
		– **Yes** is set under "Allow TCP connections upon SYN only"
		– The firewall rules have been adjusted
		– The value was changed from **No** to **Yes** (even without changing the firewall rules)
		After changing the firewall rules, the FL MGUARD behaves like after a restart. However, this only applies to the forwarded connections. Existing TCP connections are interrupted, even if they are allowed according to the new firewall rules. Connections to the device are not affected, even if the firewall rules have been changed for the remote access.
		If set to **No**, the connections remain, even if the firewall rules changed would not allow or abort them.
	FT	**Yes/No**
		If an outgoing connection is established to call data for the FTP protocol, two methods of data transmission can be used:
		With "active FTP", the called server establishes an additional counter-connection to the caller in order to transmit data over this connection.
		With "passive FTP", the client establishes this additional connection to the server for data transmission.
		FTP must be set to **Yes** (default) so that additional connections can pass through the firewall.
	IRC	**Yes/No**
		Similar to FTP: For IRC chat over the Internet to work properly, incoming connections must be allowed following active connection establishment. IRC must be set to **Yes** (default) in order for these connections to pass through the firewall.
	PPTP	**Yes/No, default: No**
		Must be set to **Yes** if VPN connections are to be established using PPTP from local computers to external computers without the assistance of the FL MGUARD.
		Must be set to **Yes** if GRE packets are to be forwarded from the internal area to the external area.
	H.323	**Yes/No, default: No**
		Protocol used to establish communication sessions between two or more devices. Used for audio-visual transmission. This protocol is older than SIP.

Network Security >> Packet Filter >> Advanced [...]

	SIP	**Yes/No, default: No**
		SIP (Session Initiation Protocol) is used to establish communication sessions between two or more devices. Often used in IP telephony.
		When set to **Yes**, it is possible for the FL MGUARD to track the SIP and add any necessary firewall rules dynamically if further PCP channels are established to the same session.
		When NAT is also activated, one or more locally connected computers can communicate with external computers by SIP via the FL MGUARD.

5.5.1.6   Firewall on FL MGUARD RS2000

ℹ   The FL MGUARD RS2000 has a simple "2-click firewall". This either permits or rejects all incoming and outgoing connections. No advanced settings are provided. Furthermore, access via this firewall is not logged (see Section 5.11.2, *Logging >> Browse local logs*).

The following firewall functionality is available when using the **FL MGUARD RS2000**:
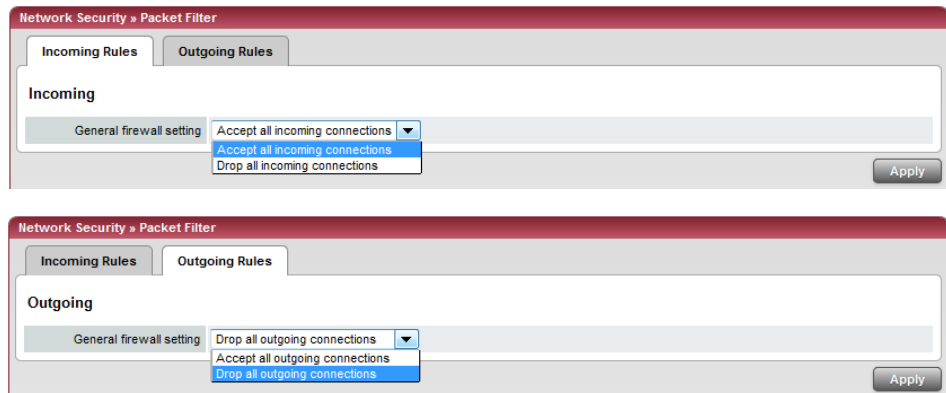
These variables are also available on other devices. However, other devices also have advanced settings (see "Incoming Rules" on page 180 and "Outgoing Rules" on page 182).

5.5.2 Network Security >> DoS Protection

5.5.2.1 Flood Protection

ℹ️ This menu is **not** available on the **FL MGUARD RS2000**.

Network Security >> DoS Protection >> Flood Protection		
TCP	**Maximum number of new incoming/ outgoing TCP connections (SYN) per second**	Outgoing: Default setting: 75
		Incoming: Default setting: 25
		Maximum values for the number of incoming and outgoing TCP connections allowed per second.
		These values are set to a level that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection.
		If there are special requirements in your operating environment, these values can be increased.

Network Security >> DoS Protection >> Flood Protection [...]		
ICMP	**Maximum number of incoming/outgoing "ping" frames (ICMP Echo Request) per second**	Outgoing: Default setting: 5
		Incoming: Default setting: 3
		Maximum values for the number of incoming and outgoing "ping" packets allowed per second.
		These values are set to a level that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection.
		If there are special requirements in your operating environment, these values can be increased.
		Value **0** means that no "ping" packets are allowed through or in.
Stealth Mode	**Maximum number of incoming/outgoing ARP requests or ARP replies per second each**	Default setting: 500
		Maximum values for the number of incoming and outgoing ARP requests allowed per second.
		These values are set to a level that can never be reached during normal practical operation. However, they can be easily reached in the event of attacks, thus providing additional protection.
		If there are special requirements in your operating environment, these values can be increased.

5.5.3 Network Security >> User Firewall

The user firewall is used exclusively by firewall users, i.e., users that are registered as firewall users (see "Authentication >> Firewall Users" on page 159).

Each firewall user can be assigned a set of firewall rules, also referred to as a template.

5.5.3.1 User Firewall Templates

All defined user firewall templates are listed here. A template can consist of several firewall rules. A template can be assigned to several users.

Defining a new template:

- In the template table, click on **Edit** to the right of the "(unnamed)" entry under "Name".
- If the "(unnamed)" entry cannot be seen, open another row in the table.

Editing a set of rules:

- Click on **Edit** to the right of the relevant entry.

Network Security >> User Firewall >> User Firewall Templates		
General	**Enabled**	Activates/deactivates the relevant template.
	Name	Name of the template. The name is specified when the template is created.
	The following tab page appears when you click on **Edit**:	
Options	**A descriptive name for the template**	The user firewall template can be freely named and renamed.
	Enabled	**Yes/No**
		When set to **Yes**, the user firewall template becomes active as soon as firewall users log into the FL MGUARD who are listed on the *Template users* tab page (see below) and who have been assigned this template. It does not matter from which computer and under what IP address the user logs in. The assignment of the firewall rules to a user is based on the authentication data that the user enters during login (user name, password).
	Comment	Optional explanatory text.

Network Security >> User Firewall >> User Firewall Templates [...]		
	Timeout	Default: 28800.
		Specifies the time in seconds at which point the firewall rules are deactivated. If the user session lasts longer than the timeout time specified here, the user has to log in again.
	Timeout type	static/dynamic
		With a *static* timeout, users are logged out automatically as soon as the set timeout time has elapsed. With *dynamic* timeout, users are logged out automatically after all the connections have been closed by the user or have expired on the FL MGUARD, and the set timeout time has elapsed.
		An FL MGUARD connection is considered to have expired if no more data is sent for this connection over the following periods.
	Connection expiration period after non-usage	
	– TCP	5 days (this value can be set, see 5-190.) 120 seconds are added after closing the connection. (This also applies to connections closed by the user.)
	– UDP	30 seconds after data traffic in one direction 180 seconds after data traffic in both directions
	– ICMP	30 seconds
	– Others	10 minutes

Network Security >> User Firewall >> User Firewall Templates >> Edit > ...

Template users	

Network Security » User Firewall » BluePrint

| General | **Template users** | Firewall rules |

Users
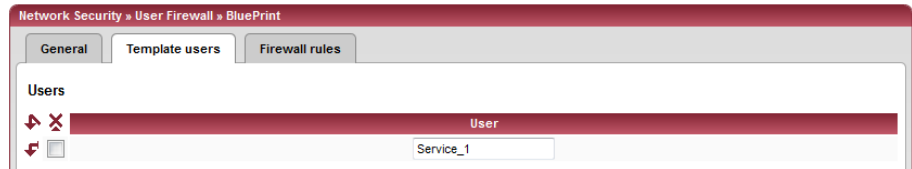
| ↴ ✖ | | **User** |
| ↴ ☐ | | Service_1 |

Specify the names of the users here. The names must correspond to those that have been defined under the Authentication >> Firewall Users menu (see Page 159).

Firewall rules

Network Security » User Firewall » BluePrint

| General | Template users | **Firewall rules** |

Firewall rules

| Source IP | %authorized_ip |

Log ID: ufw—N°-24dfa322-3649-14fc-b355-000cbe0600f0

↴ ✖	N°	Protocol	From Port	To IP	To Port	Comment	Log
↴ ☐	1	TCP ▾	any	0.0.0.0/0	any	important!	Yes ▾
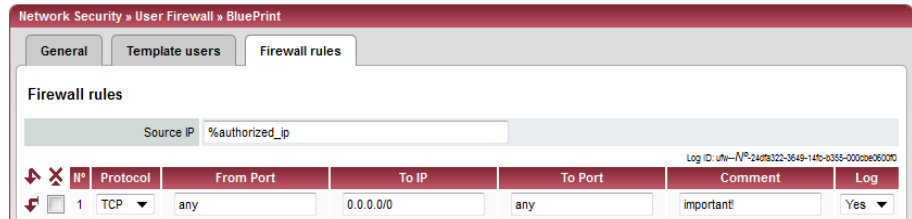
Source IP IP address from which connections are allowed to be established. If this should be the address from which the user logged into the FL MGUARD, the wildcard "%authorized_ip" should be used.

> ℹ️ If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

Protocol **All** means TCP, UDP, ICMP, GRE, and other IP protocols

From Port/To Port (Only evaluated for TCP and UDP protocols.)
– **any** refers to any port.
– **startport:endport** (e.g., 110:120) > port area.

Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).

To IP **0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).

Comment Freely selectable comment for this rule.

Log For each firewall rule, you can specify whether the use of the rule:
– Should be logged – set *Log* to **Yes**
– Should not be logged – set *Log* to **No** (default setting)

5.6 CIFS Integrity Monitoring menu

i	CIFS integrity monitoring is **not** available on the **FL MGUARD RS2000**.

i	In Stealth network mode, CIFS integrity checking is not possible without a management IP address and the CIFS server for the anti-virus scan is not supported.

There are two options for checking network drives for viruses using CIFS integrity monitoring.

– CIFS Integrity Checking
– CIFS Antivirus Scan Connector

CIFS Integrity Checking

When **CIFS integrity checking** is performed, the Windows network drives are checked to determine whether certain files (e.g., *.exe, *.dll) have been changed. Changes to these files indicate a possible virus or unauthorized intervention.

CIFS Antivirus Scan Connector

The **CIFS Antivirus Scan Connector** enables the FL MGUARD to perform a virus scan on drives that are otherwise not externally accessible (e.g., production cells). The FL MGUARD mirrors a drive externally in order to perform the virus scan. Additional anti-virus software is required for this procedure. Set the necessary read access for your anti-virus software.

Setting options for CIFS integrity checking

– Which network drives are known to the FL MGUARD (see "CIFS Integrity Monitoring >> Importable Shares" on page 200).
– What type of access is permitted (see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings" on page 201).
– At what intervals the drives should be checked (see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit" on page 203).
– Which file types should be checked (see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns" on page 205).
– Warning method when a change is detected (e.g., via e-mail, see "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings" on page 201 or via SNMP, see "CIFS integrity traps" on page 95).

Setting options for CIFS anti-virus scan connector

– Which network drives are known to the FL MGUARD (see "CIFS Integrity Monitoring >> Importable Shares" on page 200).
– What type of access is permitted (read or read/write access, see "CIFS Integrity Monitoring >> CIFS AV Scan Connector" on page 210).

5.6.1 CIFS Integrity Monitoring >> Importable Shares

Requirements: The network drives that the FL MGUARD should check regularly can be specified here.

> [i] In order for the network drives to be checked, you must also refer to these network drives in one of the two methods (CIFS integrity checking or CIFS anti-virus scan connector).

The references to the network drives can be set as follows:

5.6.1.1 Importable Shares

CIFS Integrity Monitoring >> Importable Shares			
Importable CIFS Shares	**Name**		Name of the network drive to be checked (internal name used in the configuration).
	Server		IP address of the authorizing server.
	Share		Name of the network drive made available by the authorizing server. Click on **Edit** to make the settings.

CIFS Integrity Monitoring >> Importable Shares >> Edit		
Identification for Reference	**Name**	Name of the network drive to be checked (internal name used in the configuration).
Location of the Importable Share	**IP address of the server**	IP address of the server whose network drive is to be checked.
	Imported share's name	Directory on the above authorized server that is to be checked.

CIFS Integrity Monitoring >> Importable Shares >> Edit [...]		
Authentication for mounting the Share	**Workgroup**	Name of the workgroup to which the network drive belongs.
	Login	Login for the server.
	Password	Password for login.

5.6.2 CIFS Integrity Monitoring >> CIFS Integrity Checking

When **CIFS integrity checking** is performed, the Windows network drives are checked to determine whether certain files (e.g., *.exe, *.dll) have been changed. Changes to these files indicate a possible virus or unauthorized intervention.

Integrity database

If a network drive that is to be checked is reconfigured, an integrity database must be created.

This integrity database is used as the basis for comparison when checking the network drive regularly. The checksums of all files to be monitored are recorded here. The integrity database is protected against manipulation.

The database is either created explicitly due to a specific reason (see "CIFS Integrity Monitoring >> CIFS Integrity Status >> Show >> Actions" on page 208) or on the first regular check of the drive.

i	The integrity database must be created again following intentional manipulation of the relevant files of the network drive. Unauthorized manipulation of the relevant files cannot be detected if there is no (valid) integrity database.

5.6.2.1 Settings

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings		
General	**Integrity certificate (Used to sign integrity databases.)**	Used for signing and checking the integrity database so that it cannot be replaced or manipulated by an intruder without being detected.
		For information about certificates, please refer to "Machine certificates" on page 171.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings [...]		
	Send notifications via e-mail	**After every check**: An e-mail is sent to the address specified below after every check.
		No: An e-mail is not sent to the address specified below.
		Only with faults and deviations: An e-mail is sent to the address specified below if a deviation is detected during CIFS integrity checking or if the check could not be carried out due to an access error.
	Target address for e-mail notifications	An e-mail is sent to this address either after every check or only if a deviation is detected during CIFS integrity checking or if the check could not be carried out due to an access error.
	Sender address of e-mail notifications	This address is entered as the sender in the e-mail.
	Address of the e-mail server	IP address or host name of the e-mail server via which the e-mail is sent.
	Subject prefix for e-mail notifications	Text entered in the subject field of the e-mail.
Checking of Shares	**Enabled**	**No**: A check is not triggered for this network drive. The FL MGUARD has not connected this drive. The status cannot be viewed.
		Yes: A check is triggered regularly for this network drive.
		Suspended: The check has been suspended until further notice. The status can be viewed.
	Checked CIFS Share	Name of the network drive to be checked (specified under *CIFS Integrity Monitoring >> Importable Shares >> Edit*).
	Checksum Memory	In order to perform the check, the FL MGUARD must be provided with a network drive for storing the files.
		The checksum memory can be accessed via the external network interface.
	Click on **Edit** to make further settings for checking network drives.	

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit		
Settings	**Enabled**	**No**: A check is not triggered for this network drive. The FL MGUARD has not connected this drive. The status cannot be viewed.
		Yes: A check is triggered regularly for this network drive.
		Suspended: The check has been suspended until further notice. The status can be viewed.
	Checked CIFS Share	Name of the network drive to be checked (specified under *CIFS Integrity Monitoring >> Importable Shares >> Edit*).
	Patterns for filenames	Specific file types are checked (e.g., only executable files such as *.exe and *.dll).
		The rules can be defined under *CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns* .
		Do not check files that are changed in normal operation, as this could trigger false alarms.
		Do not check files that are simultaneously opened **exclusively** by other programs, as this can lead to access conflicts.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit [...]

	Time Schedule	Everyday, Mondays, Tuesdays, etc. at xx h, xx m
		You can start a check every day or on a specific weekday at a specific time (hours, minutes).
		The FL MGUARD system time must be set for the time schedule to work properly. Integrity checks are not performed if the system time is not synchronized. This can be carried out manually or via NTP (see "Time and Date" on page 53).
		A check is only started if the FL MGUARD is operating at the set time. If the FL MGUARD is not operating at the time, a check is not performed later when the FL MGUARD is started up again.
		The check can also be started manually ("CIFS Integrity Monitoring >> CIFS Integrity Status >> Show >> Actions" on page 208).
	Maximum time a check may take	Maximum duration of the check sequence in minutes.
		You can thus ensure that the check is completed in good time (e.g., before a shift starts).
Checksum Memory	**Checksum Algorithm**	**SHA-1**
		MD5
		SHA-256
		Checksum algorithms such as MD5, SHA-1 or SHA-256 are used to check whether a file has been changed.
		SHA-256 is more secure than SHA-1, but it takes longer to process.
	To be stored on CIFS share	In order to perform the check, the FL MGUARD must be provided with a network drive for storing the files.
		The checksum memory can be accessed via the external network interface.
		The same network drive can be used as the checksum memory for several different drives to be checked. The base name of the checksum files must then be clearly selected in this case.
		The FL MGUARD recognizes which version the checksum files on the network drive must have.
		For example, if it is necessary to restore the contents of the network drive from a backup following a malfunction, old checksum files are provided in this case and the FL MGUARD would detect the deviations. In this case, the integrity database must be recreated (see "CIFS Integrity Monitoring >> CIFS Integrity Status >> Show >> Actions" on page 208).

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit [...]

	Basename of the checksum files (May be prefixed with a directory.)	The checksum files are stored on the network drive specified above. They can also be stored in a separate directory. The directory name must not start with a backslash (\).

Example: Checksumdirectory\integrity-checksum

"Checksumdirectory" is the directory and contains the files beginning with "integrity-checksum". |

5.6.2.2 Patterns for filenames
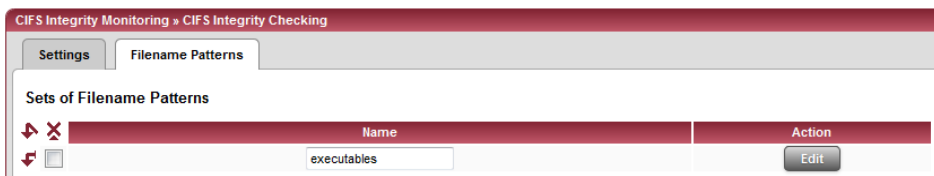
CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns

| **Sets of Filename Patterns** | **Name** | Freely definable name for a set of rules for the files to be checked.

This name must be selected under **CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit** in order for the sample to be activated.

Click on **Edit** to define a set of rules for the files to be checked and save this under the defined name. |
|---|---|---|

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns >> Edit		
Rules for files to check	**Filename pattern**	The following rules apply:
		***.exe means that the files located in a specific directory and with file extension **.exe* are checked (or excluded).
		Only one wildcard (*) is permitted per directory or file name.
		Wildcards represent characters, e.g., *win**.exe* returns files with the extension **.exe* that are located in a directory that begins with *win...*
		** at the start means that any directory is searched, even those at the top level (if this is empty). This cannot be combined with other characters (e.g., *c*** is not permitted).
		Example: *Name***.exe* refers to all files with the extension **.exe* that are located in the "*Name*" directory and any subdirectories.
		i Missing files trigger an alarm. Missing files are files that were present during initialization. An alarm is also triggered if additional files are present.
	Include in check	**Include**: The files are included in the check.
		(Each file name is compared with the samples one after the other. The first hit determines whether the file is to be included in the integrity check. The file is not included if no hits are found.)
		Exclude: The files are excluded from the check.

5.6.3 CIFS Integrity Monitoring >> CIFS Integrity Status

CIFS Integrity Monitoring >> CIFS Integrity Status	
List with buttons for each individual network drive	
Checked CIFS Share	Click on **Show** to see the result of the check or to carry out actions (such as start or cancel check, update integrity database if the network drives to be checked have been intentionally changed).
	Click on **Edit** to revise the settings for the check (same as "CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit" on page 203).
Status Summary	Result and time of the last checks.
Click on **Update** to see a summary of the results of the latest checks.	
Update applies to all network drives.	

CIFS Integrity Monitoring >> CIFS Integrity Status >> Show >> Status		
Status of [network drive name according to configuration]	**Summary**	**Last check was OK**: No deviations found.
		Last check found x deviation(s): The exact deviations are listed in the check report.
	Report	The check report is displayed here. It can be downloaded by clicking on **Download the report**.
	UNC notation of the imported share	\\Servername\networkdrive\

CIFS Integrity Monitoring >> CIFS Integrity Status >> Show >> Status [...]		
	Start of the last check	Weekday, month, day, HH:MM:SS (UTC).
		The local time may differ from this time.
		Example: The standard time in Germany is Central European Time (CET), which is UTC plus one hour. Central European Summer Time applies in summer, which is UTC plus two hours.
	Duration of the last check	Duration of the check in hours and minutes.
		(Only displayed if a check has been carried out.)
	Start of the current check	See "Start of the last check" on page 208
		(Only displayed if a check has been carried out.)
	Progress of the current check	Only displayed if a check is currently active.

CIFS Integrity Monitoring >> CIFS Integrity Status >> Show >> Actions		
Possible Actions for ...	**Verify the validity of the recent check report**	Click on **Validate the report** to check whether the report is unchanged from the definition in the FL MGUARD (according to the signature and certificate).
	Start an integrity check right now	Click on **Start a check** to start the integrity check.
		Only displayed if a check is not currently active.
	Cancel the currently running integrity check	Click on **Cancel** to stop the integrity check.
		Only displayed if a check is currently active.

CIFS Integrity Monitoring >> CIFS Integrity Status >> Show >> Actions [...]		
	(Re-)Build the integrity database	The FL MGUARD creates a database with checksums in order to check whether files have been changed. A change to executable files indicates a virus.
		However, if these files have been changed intentionally, a new database must be created by clicking on **Initialize** in order to prevent false alarms.
		The creation of an integrity database is also recommended if network drives have been newly set up. Otherwise, an integrity database is set up during the first scheduled check instead of a check being performed.
	Cancel the creation of the integrity database **Only displayed when a database is being created.**	Click **Cancel** to stop the creation of the integrity database.
		The old database is no longer used. A new database must be created manually, otherwise it is created automatically on the next scheduled check of the drive.
		The contents of the drive may be manipulated (e.g., infected) without being detected if no integrity database is in place.
	Erase reports and the integrity database	Click on **Erase** to delete all existing reports/databases.
		A new integrity database must be created for any further integrity checks. This can be initiated by clicking on **Initialize.** Otherwise, a new integrity database is created automatically upon the next scheduled check. This procedure cannot be seen.

5.6.4 CIFS Integrity Monitoring >> CIFS AV Scan Connector

i	In Stealth network mode without management IP address, the CIFS server for the anti-virus scan is not supported.

CIFS Antivirus Scan Connector

The **CIFS Antivirus Scan Connector** enables the FL MGUARD to perform a virus scan on drives that are otherwise not externally accessible (e.g., production cells). The FL MGUARD mirrors a drive externally in order to perform the virus scan. Additional anti-virus software is required for this procedure. Set the necessary read access for your anti-virus software.

5.6.4.1 CIFS Antivirus Scan Connector

CIFS Integrity Monitoring >> CIFS AV Scan Connector		
CIFS Server	**Enable the server**	**No**: CIFS server is not available
		Yes: CIFS server is available

CIFS Integrity Monitoring >> CIFS AV Scan Connector [...]		
	Accessible as	Displays the virtual network drive provided by the FL MGUARD for the "CIFS Antivirus Scan Connector" function.
		This path is displayed with UNC notation. By means of copy and paste, it can be directly used on the PC which is to use the virtual network drive (see"Accessing the virtual network (CIFS Antivirus Scan Connector)" on page 213).
		Two UNC addresses (for the internal and external interface) are displayed in "Router" network mode, while one UNC address is displayed in "Stealth" network mode.
		Access to the virtual network drive can be prevented as a result of the settings in the "Allowed Networks" section. Enter a rule here accordingly, especially if access via the external interface is required.
		Depending on the FL MGUARD configuration, further access options can be established over other IP addresses, such as access via VPN channels or via incoming calls (for dial-in, see "Dial-in" on page 136).
	Server's workgroup	Name of the CIFS server workgroup.
	Login	Login for the server.
	Password	Password for login.
	Exported share's name	Name for the computers that are to use the CIFS server to access the combined drives (the drives are connected under this name).
	Allow write access	**No**: Read-only access
		Yes: Read and write access
Allowed Networks		These rules allow external access to the CIFS server of the FL MGUARD.
		In Router mode with NAT or port forwarding, the port numbers for the CIFS server have priority over the rules for port forwarding (port forwarding is set under "Network >> NAT").
		Access to the CIFS server is approved internally via incoming calls (dial-in) and VPN as standard, and can be restricted or expanded via the firewall rules. A different default setting can also be defined using these rules.
	From IP	Enter the address of the computer/network from which remote access is permitted or forbidden in this field.
		IP address **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format (see 5-294).

CIFS Integrity Monitoring >> CIFS AV Scan Connector [...]			
	Interface	**External/Internal/External 2/VPN/Dial-in**[1]	
		Specifies to which interface the rule should apply.	
		If no rules are set or if no rule applies, the following default settings apply: – Remote access is permitted via *Internal*, *VPN*, and *Dial-in.* – Access via *External* and *External 2* is refused.	
		Specify the access options according to your requirements.	
		If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action.	
	Action	**Accept** means that the data packets may pass through.	
		Reject means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, Reject has the same effect as Drop.)	
		Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.	
	Comment	Freely selectable comment for this rule.	
	Log	For each individual rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default settings).	
Consolidated Imported Shares	**Enabled**	**No**: This network drive is not mirrored.	
		Yes: This network drive is mirrored and made available.	
	Exported in Subdirectory	Several drives can be combined as one in this directory.	
	CIFS Share	Name of the network drive to be imported (created under *CIFS Integrity Monitoring >> Importable Shares >> Edit*).	

[1] *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 104).

Accessing the virtual network (CIFS Antivirus Scan Connector)

The virtual network drive provided by the FL MGUARD for the CIFS Antivirus Scan Connector can be integrated in Windows Explorer. To do this, open the "Tools, Map Network Drive..." menu in Windows Explorer and enter the path using UNC notation.

This path is displayed under "CIFS Integrity Monitoring >> CIFS AV Scan Connector >> Accessible as".

\\<External IP of FL MGUARD>\<Name of the exported share>
\\<Internal IP of FL MGUARD>\<Name of the exported share>

Example

\\10.1.66.49\exported-av-share

\\192.168.66.49\exported-av-share

Alternatively, you can enter the "net use" command in the command line. For further information, please refer to the Microsoft product information.

Notes

– DNS names can also be used instead of the IP address.
– The authorized network cannot be found using the browse or search function.
– The "Exported share's name" must always be added.
– Windows does not automatically display the authorized network drive upon connection of the FL MGUARD.

5.7   IPsec VPN menu

5.7.1   IPsec VPN >> Global

5.7.1.1   Options

IPsec VPN >> Global >> Options			
Options	**Allow packet forwarding between VPN connections**	**i**	This option should only be set to **Yes** on an FL MGUARD communicating between two different VPN partners.
		i	To enable communication between two VPN partners, the local network of the communicating FL MGUARD must be configured so that the remote networks containing the VPN partners are included. The opposite setup (local and remote network swapped round) must also be implemented for VPN partners (see "Remote" on page 228).
		i	**Yes** is not supported in *Stealth* network mode.

IPsec VPN >> Global >> Options [...]		
		No (default): VPN connections exist separately.
		Yes: Hub and spoke feature enabled: A control center diverts VPN connections to several branches that can also communicate with each other.
		With a star VPN connection topology, FL MGUARD partners can also exchange data with one another. In this case, it is recommended that the local FL MGUARD consults CA certificates for the authentication of partners (see "Authentication" on page 237).
	Archive diagnostic messages for VPN connections: No/Only when started via nph-vpn.cgi or CMD contact The CMD contact is only available on the FL MGUARD RS4000/2000.	If errors occur when establishing VPN connections, the FL MGUARD logging function can be used to find the source of the error based on corresponding entries (see *Logging >> Browse local logs* menu item). This option for error diagnostics is used as standard. Set this option to **No** (default) if it is sufficient.
Option	**Only when started via nph-vpn.cgi or CMD contact:**	

If the option of diagnosing VPN connection problems using the FL MGUARD logging function is too impractical or insufficient, select this option. This may be the case if the following conditions apply:

– In certain application environments, e.g., when the FL MGUARD is "operated" by means of a machine controller via the CMD contact (*FL MGUARD RS4000/2000* only), the option for a user to view the FL MGUARD log file via the web-based user interface of the FL MGUARD may not be available at all.

– If the FL MGUARD is being used remotely, it is possible that a VPN connection error can only be diagnosed after the FL MGUARD is temporarily disconnected from its power source – which causes all the log entries to be deleted.

– The relevant log entries of the FL MGUARD that could be useful may be deleted because the FL MGUARD regularly deletes older log entries on account of its limited memory space.

– If an FL MGUARD is being used as the central VPN partner, e.g., in a remote maintenance center as the gateway for the VPN connections of numerous machines, the messages regarding activity on the various VPN connections are logged in the same data stream. The resulting volume of the logging makes it time-consuming to find the information relevant to one error.

After archiving is enabled, relevant log entries about the operations involved in establishing VPN connections are archived in the non-volatile memory of the FL MGUARD if the connections are established as follows:

– Via the CMD contact

– Via the CGI interface nph-vpn.cgi using the "synup" command (see *Application Note: Diagnosis of VPN connections*). (Application notes are available in the download area at innominate.com.)

Archived log entries are not affected by a restart. They can be downloaded as part of the support snapshot (*Support >> Advanced* menu item, *Snapshot* tab page). A snapshot provides your dealer's support team with additional options for more efficient troubleshooting than would be possible without archiving.

IPsec VPN >> Global >> Options [...]		
	Archive diagnostic messages only upon failure: Yes/No	Only visible if archiving is enabled. If only log entries generated for failed connection attempts are to be archived, set this option to **Yes**. If set to **No**, all log entries will be archived.
VPN Switch FL MGUARD RS4000/ RS2000 only.	**VPN connection**	The FL MGUARD RS4000/RS2000 devices have connections to which an external button or on/off switch and a signal LED can be connected. One of the configured VPN connections can be established and released via the button or on/off switch. The VPN connection is specified here.
		If VPN connections are configured and listed under the *IPsec VPN >> Connections* menu item (see Page 222), they are displayed in this selection list. Select here if the connection is to be established or released manually by pressing the button or switch.
		<table><tr><td>**i**</td><td>If starting and stopping the VPN connection via the CMD contact is enabled, only the CMD contact is authorized to do this. This means that setting this option to Enabled for the entire VPN connection has no effect. If a button is connected to the CMD contact (instead of a switch – see below), the connection can also be established and released using the CGI script command nph-vpn.cgi, which has the same rights.</td></tr></table>
		When set to **Off**, this function is disabled. If a button or on/off switch is connected to the FL MGUARD service contacts, then pressing it has no effect.
		<table><tr><td>**i**</td><td>*If a VPN connection is controlled via a VPN switch, then VPN redundancy cannot be activated.*</td></tr></table>

IPsec VPN >> Global >> Options [...]		
FL MGUARD RS4000/ RS2000 only.	**Switch type connected to the contact**	**Pushbutton or on/off switch** The FL MGUARD RS4000/RS2000 devices have connections to which an external button/switch and a signal LED can be connected. Select the switch type that is connected to the corresponding service contacts of the FL MGUARD. For more information, see – "Installing the FL MGUARD RS4000/RS2000" on page 20 under **Service contacts**. Information about how to operate the different switch types is also provided.

> **i** If a VPN connection is established by pressing the button or switch, the connection is maintained until it is released by pressing the button or switch again.

> **i** If an on/off switch is used (instead of a button) and it is pressed to establish a VPN connection, this connection is reestablished automatically when the FL MGUARD is restarted.

TCP Encapsulation

This function is used to encapsulate data packets to be transmitted via a VPN connection in TCP packets. Without this encapsulation, it is possible for VPN connections that under certain circumstances important data packets belonging to the VPN connection may not be correctly transmitted due to interconnected NAT routers, firewalls or proxy servers, for example.

Firewalls, for example, may be set up to prevent any data packets of the UDP protocol from passing through or (incorrectly implemented) NAT routers may not manage the port numbers correctly for UDP packets.

TCP encapsulation avoids these problems because the packets belonging to the relevant VPN connection are encapsulated in TCP packets, i.e., they are hidden so that only TCP packets appear for the network infrastructure.

The FL MGUARD may receive VPN connections encapsulated in TCP, even when the FL MGUARD is positioned behind a NAT gateway in the network and thus cannot be reached by the VPN partner under its primary external IP address. To do this, the NAT gateway must forward the corresponding TCP port to the FL MGUARD (see "Listen for incoming VPN connections, which are encapsulated" on page 219).

i	TCP encapsulation can only be used if an FL MGUARD (Version 6.1 or later) is used at both ends of the VPN tunnel.

i	TCP encapsulation should only be used if required because connections are slowed down by the significant increase in the data packet overhead and by the correspondingly longer processing times.

i	If the FL MGUARD is configured to use a proxy for HTTP and HTTPS in the "Network >> Proxy Settings" menu item, then this proxy is also used for VPN connections that use TCP encapsulation.

i	TCP encapsulation supports the *basic authentication* and *NTLM* authentication methods for the proxy.

i	For the TCP encapsulation to work through an HTTP proxy, the proxy must be named explicitly in the proxy settings ("Network >> Proxy Settings" menu item) (i.e., it must not be a transparent proxy) and this proxy must also understand and permit the HTTP method CONNECT.

As participants in the TCP encapsulation, the FL MGUARD devices for the machine control systems initiate VPN data traffic to the maintenance center and encapsulate the data packets sent to it.

As soon as a connection is initiated, the maintenance center also automatically encapsulates the data packets sent to the relevant VPN partner.
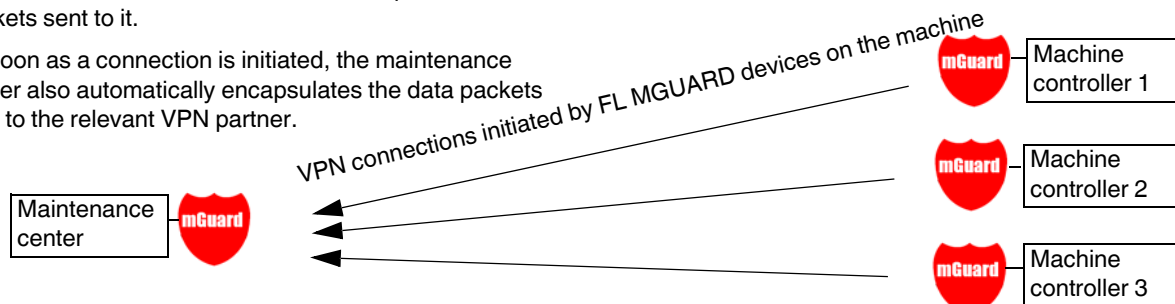
FL MGUARD of maintenance center

Required basic settings
– **IPsec VPN** menu item, *Global*, *Options* tab page:
Listen for incoming VPN connections, which are encapsulated: **Yes**
– *Connections* submenu,
General tab page:
Address of the partner's VPN gateway: **%any**
Connection startup: **Wait**

FL MGUARD devices on machine control systems

Required basic settings
– **IPsec VPN** menu item, *Global*, *Options* tab page:
Listen for incoming VPN connections, which are encapsulated: **No**
– *Connections* submenu, *General* tab page:
Address of the partner's VPN gateway: Fixed IP address or host name
Connection startup: **Initiate** or **Initiate on traffic**
Encapsulate the VPN traffic in TCP: **Yes**

Figure 5-2 TCP encapsulation in an application scenario with a maintenance center and machines maintained remotely via VPN connections

IPsec VPN >> Global >> Options		
TCP Encapsulation	**Listen for incoming VPN connections, which are encapsulated**	Default setting: **No** Only set this option to **Yes** if the TCP Encapsulation function is used. Only then can the FL MGUARD allow connection establishment with encapsulated packets.
		For technical reasons, the main memory (RAM) requirements increase with each interface that is used to listen out for VPN connections encapsulated in TCP. If multiple interfaces need to be used for listening, then the device must have at least 64 Mbytes RAM.
		The interfaces to be used for listening are determined by the FL MGUARD according to the settings on the active VPN connections that have "%any" configured as the partner. The decisive setting is specified under "Interface to use for gateway setting %any".

IPsec VPN >> Global >> Options [...]		
	TCP port to listen on	Number of the TCP port where the encapsulated data packets to be received arrive. The port number specified here must be the same as the one specified for the FL MGUARD of the partner as the **TCP port of the server, which accepts the encapsulated connection** (*IPsec VPN >> Connections* , Edit menu item, *General* tab page).
		The following restriction applies:
		– The port to be used for listening must not be identical to a port that is being used for remote access (SSH, HTTPS).
	Server ID (0-63)	Usually, the default value **0** does not have to be changed. The numbers are used to differentiate between different control centers.
		A different number is only to be used in the following scenario: An FL MGUARD connected upstream of a machine must establish connections to two or more different maintenance centers and their FL MGUARD devices with TCP encapsulation enabled.
IP Fragmentation	**IKE Fragmentation**	UDP packets can be oversized if an IPsec connection is established between the participating devices via IKE and certificates are exchanged. Some routers are not capable of forwarding large UDP packets if they are fragmented over the transmission path (e.g., via DSL in 1500-byte segments). Some faulty devices forward the first fragment only, resulting in connection failure.
		If two FL MGUARD devices communicate with each other, it is possible to ensure at the outset that only small UDP packets are to be transmitted. This prevents packets from being fragmented during transmission, which can result in incorrect routing by some routers.
		If you want to use this option, set it to **Yes**.
		i If this option is set to **Yes**, the setting only takes effect if the remote peer is an FL MGUARD with installed firmware Version 5.1.0 or later. In all other cases, the setting has no effect, negative or otherwise.
	IPsec MTU (default is 16260)	The option for avoiding oversized IKE data packets, which cannot be routed correctly on the transmission path by faulty routers, can also be applied for IPsec data packets. In order to remain below the upper limit of 1500 bytes often set by DSL, it is recommended that a value of 1414 (bytes) be set. This also allows enough space for additional headers.
		If you want to use this option, specify a value lower than the default setting.

5.7.1.2 DynDNS Monitoring

For an explanation of DynDNS, see "DynDNS" on page 150.

IPsec VPN >> Global >> Options		
DynDNS Monitoring	**Watch hostnames of remote VPN Gateways?**	**Yes/No**
		If the FL MGUARD knows the address of a VPN partner in the form of a host name (see "Defining a VPN connection/VPN connection channels" on page 223) and this host name is registered with a DynDNS service, then the FL MGUARD can check the relevant DynDNS at regular intervals to determine whether any changes have occurred. If so, the VPN connection will be established to the new IP address.
	Refresh Interval (sec)	Default: 300

5.7.2 IPsec VPN >> Connections

Requirements for a VPN connection

A general requirement for a VPN connection is that the IP addresses of the VPN partners are known and can be accessed.

– FL MGUARDs provided in stealth network mode are preset to the "multiple clients" stealth configuration. In this mode, you need to configure a management IP address and default gateway if you want to use VPN connections (see Page 114). Alternatively, you can select a different stealth configuration than the "multiple clients" configuration or use another network mode.

– In order to successfully establish an IPsec connection, the VPN partner must support IPsec with the following configuration:

  – Authentication via pre-shared key (PSK) or X.509 certificates
  – ESP
  – Diffie-Hellman group 2 or 5
  – DES, 3DES or AES encryption
  – MD5, SHA-1 or SHA-2 hash algorithms
  – Tunnel or transport mode
  – Quick mode
  – Main mode
  – SA lifetime (1 second to 24 hours)

  If the partner is a computer running Windows 2000, the *Microsoft Windows 2000 High Encryption Pack* or at least *Service Pack 2* must be installed.

– If the partner is positioned downstream of a NAT router, the partner must support NAT-T. Alternatively, the NAT router must know the IPsec protocol (IPsec/VPN passthrough). For technical reasons, only IPsec tunnel connections are supported in both cases.

5.7.2.1 Connections

Lists all the VPN connections that have been defined.

Each connection name listed here can refer to an individual VPN connection or a group of VPN connection channels. You have the option of defining several tunnels under the transport and/or tunnel settings of the relevant entry.

You also have the option of defining new VPN connections, activating and deactivating VPN connections, changing (editing) the VPN connection or connection group properties, and deleting connections.

IPsec VPN » Connections		
Connections		
Enabled	Name	Action
Yes ▼	Mannheim-Leipzig	Edit
Yes ▼	MA-Techniker-Zentrale	Edit
Yes / No		
		Apply

Defining a new VPN connection/VPN connection channels:

• In the connections table, click on **Edit** to the right of the "(unnamed)" entry under "Name".
• If the "(unnamed)" entry cannot be seen, open another row in the table.

Editing a VPN connection/VPN connection channels:

• Click on **Edit** to the right of the relevant entry.

URL for starting, stopping, querying the status of a VPN connection

The following URL can be used to start and stop VPN connections or query their connection status, independently of their **Enabled** setting:

https://server/nph-vpn.cgi?name=verbindung&cmd=(up|down|status)

Example

wget --no-check-certificate "https://admin:FL MGUARD@192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"

The *--no-check-certificate* option ensures that the HTTPS certificate on the FL MGUARD does not undergo any further checking.

It may also be necessary to encode the password for the URL if it contains special characters.

A command like this relates to all connection channels that are grouped together under the respective name (in this example, *Athen*). This is the name entered under "A descriptive name for the connection" on the *General* tab page. In the event of ambiguity, the URL call only affects the first entry in the list of connections.

It is not possible to communicate with the individual channels of a VPN connection. If individual channels are deactivated (**Enabled**: No), they are not started. Starting and stopping in this way thus have no effect on the settings of the individual channels (i.e., the list under *Transport and Tunnel Settings*).

Starting and stopping a connection using a URL only makes sense if the connection is deactivated in the configuration (**Enabled**: No) or if **Connection startup** is set to "Wait". Otherwise, the FL MGUARD (re)establishes the connection automatically.

If the status of a VPN connection is queried using the URL specified above, then the following responses can be expected:

Table 5-1   Status of a VPN connection

Response	Meaning
unknown	A VPN connection with this name does not exist.
void	The connection is inactive due to an error, e.g., the external network is down or the host name of the partner could not be resolved in an IP address (DNS).
	"void" is also issued by the CGI interface, even if no error occurred, if, for example, the VPN connection is deactivated according to the configuration (**No** set in column) and has not been enabled temporarily using the CGI interface or CMD contact.
ready	The connection is ready to establish channels or allow incoming queries regarding channel setup.
active	At least one channel has already been established for the connection.

Defining a VPN connection/VPN connection channels

Depending on the network mode of the FL MGUARD, the following page appears after clicking on **Edit**.

5.7.2.2 General

Only in Stealth mode.

IPsec VPN >> Connections >> Edit >> General		
Options	**A descriptive name for the connection**	The connection can be freely named/renamed. If several connection channels are defined under *Transport and Tunnel Settings*, then this name applies to the entire set of VPN connection channels grouped under this name.
		Similarities between VPN connection channels:
		– Same authentication method, as specified on the *Authentication* tab page (see "Authentication" on page 237)
		– Same firewall settings
		– Same IKE options set
	Enabled	**Yes/No**
		Specifies whether the VPN connection channels defined below should all be active (Yes) or not (No).
	Address of the remote site's VPN gateway	An IP address, host name or **%any** for several partners or partners downstream of a NAT router.

Address of the remote site's VPN gateway
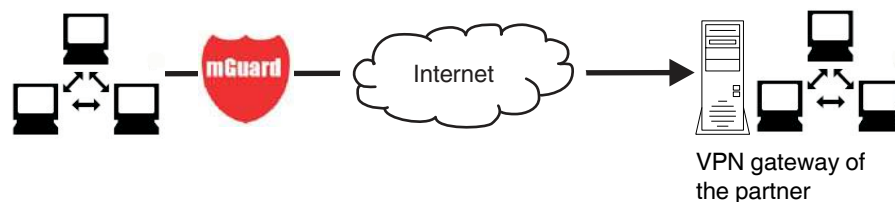
Figure 5-3   The address of the transition to the private network where the remote communication partner is located

– If the FL MGUARD should actively initiate and establish the connection to the remote partner, specify the IP address or host name of the partner here.
– If the VPN gateway of the partner does not have a fixed and known IP address, the DynDNS service (see glossary) can be used to simulate a fixed and known address.
– If the FL MGUARD should be ready to allow a connection to the local FL MGUARD that was actively initiated and established by a remote partner with any IP address, specify **%any**.

  This setting should also be selected for a VPN star configuration if the FL MGUARD is connected to the control center.

  The FL MGUARD can then be "called" by a remote partner if this partner has been dynamically assigned its IP address (by the Internet service provider), i.e., it has an IP address that changes. In this scenario, you may only specify an IP address if the remote "calling" partner has a fixed and known IP address.

i	**%any** can only be used together with the authentication method using X.509 certificates.

i	If locally stored CA certificates are to be used to authenticate the partner, the address of the VPN gateway of the partner can be specified explicitly (by means of an IP address or host name) or by **%any**. If it is specified using an explicit address (and not by "%any"), then a VPN identifier (see "VPN Identifier" on page 240) must be specified.

i	**%any** must be selected if the partner is located downstream of a NAT gateway. Otherwise, the renegotiation of new connection keys will fail on initial contact.

i	If **TCP Encapsulation** is used (see "TCP Encapsulation" on page 218): A fixed IP address or a host name must be specified if this FL MGUARD is to initiate the VPN connection and encapsulate the VPN data traffic. If this FL MGUARD is installed upstream of a maintenance center to which multiple remote FL MGUARD devices establish VPN connections and transmit encapsulated data packets, **%any** must be specified for the VPN gateway of the partner.

IPsec VPN >> Connections >> Edit >> General		
Options	Interface to use for gateway setting %any	**Internal, External, External 2, Dial-in**
		External 2 and *Dial-in* are only for devices with a serial interface, see "Network >> Interfaces" on page 104.
		Selection of the *Internal* option is not permitted in Stealth mode.
		This interface setting is only considered when "%any" is entered as the address of the VPN gateway on the partner. In this case, the interface of the FL MGUARD through which the FL MGUARD answers and permits requests for the establishment of this VPN connection is set here.
		The VPN connection can be established through the LAN and WAN port in all Stealth modes when **External** is selected.
		The interface setting allows encrypted communication to take place over a specific interface for VPN partners without a known IP address. If an IP address or host name is entered for the partner, then this is used for the implicit assignment to an interface.
		The FL MGUARD can be used as a "single-leg router" in Router mode when **Internal** is selected, as both encrypted and decrypted VPN traffic for this VPN connection is transferred over the internal interface.
		IKE and IPsec data traffic is only possible through the primary IP address of the individual assigned interface. This also applies to VPN connections with a specific partner.
	Connection startup: Initiate/Initiate on traffic/Wait	**Initiate**
		The FL MGUARD initiates the connection to the partner. In the *Address of the remote site's VPN gateway* field (see above), the fixed IP address of the partner or its name must be entered.
		Initiate on traffic
		The connection is initiated automatically when the FL MGUARD sees that the connection should be used.
		(Can be selected for all operating modes of the FL MGUARD (*Stealth*, *Router*, etc.).)
		Wait
		The FL MGUARD is ready to allow the connection to the FL MGUARD that a remote partner actively initiates and establishes.
		i If **%any** is entered under *Address of the remote site's VPN gateway*, **Wait** must be selected.

IPsec VPN >> Connections >> Edit >> General [...]

	Encapsulate the VPN traffic in TCP	**Yes/No (default: No)** If the **TCP Encapsulation** function is used (see "TCP Encapsulation" on page 218), only set this option to **Yes** if the FL MGUARD is to encapsulate its own outgoing data traffic for the VPN connection it initiated. In this case, the number of the port where the partner receives the encapsulated data packets must also be specified. When **Yes** is selected, the FL MGUARD will not attempt to establish the VPN connection using standard IKE encryption (UDP port 500 and 4500). Instead, the connection is always encapsulated using TCP.
	TCP-Port of the server, which accepts the encapsulated connection (Only visible if "Encapsulate the VPN traffic in TCP" is set to **Yes**.)	Default: **8080**. Number of the port where the encapsulated data packets are received by the partner. The port number specified here must be the same as the one specified for the FL MGUARD of the partner under **TCP port to listen on** (*IPsec VPN >> Global >> Options* menu item). **If TCP Encapsulation is used (see Page 218):** – If the FL MGUARD is to establish a VPN connection to a maintenance center and encapsulate the data traffic there: – **Initiate** or **Initiate on traffic** must be specified. – If the FL MGUARD is installed at a maintenance center to which FL MGUARD devices establish a VPN connection: – **Wait** must be specified.
Transport and Tunnel Settings Click here to specify additional tunnel and transport paths.	Stealth mode: Router mode:	

	VPN connection channels	A VPN connection defined under a descriptive name can comprise several VPN connection channels. Multiple VPN connection channels can therefore be defined here.
	For each individual VPN connection channel	When you click on **More...**, another partially overlapping page is displayed where connection parameters can be specified for the relevant transport path or tunnel.
	Enabled	**Yes/No** Specify whether the connection channel should be active (Yes) or not (No).
	Comment	Freely selectable comment text. Can be left empty.

IPsec VPN >> Connections >> Edit >> General [...]		
	Type	The following can be selected:
		– Tunnel (network ↔ network)
		– Transport (host ↔ host)
		Tunnel (network ↔ network)
		This connection type is suitable in all cases and is also the most secure. In this mode, the IP datagrams are completely encrypted and are, with a new header, transmitted to the VPN gateway of the partner – the "tunnel end". The transmitted datagrams are then decrypted and the original datagrams are restored. These are then forwarded to the destination computer.
		Transport (host ↔ host)
		For this type of connection, only the data of the IP packets is encrypted. The IP header information remains unencrypted.
		When you switch to *Transport*, the following fields (apart from Protocol) are hidden as these parameters are omitted.
	Local/Remote - for *Tunnel* **(network ↔ network)** connection type	Define the network areas for both tunnel ends under **Local** and **Remote**.
	Local	Here, specify the address of the network or computer which is connected locally to the FL MGUARD.
	Remote	Here, specify the address of the network or computer which is located downstream of the remote VPN gateway.
		If *Address of the remote site's VPN gateway* (see "Address of the remote site's VPN gateway" on page 224) is specified as **%any**, it is possible that a number of different partners will connect to the FL MGUARD.
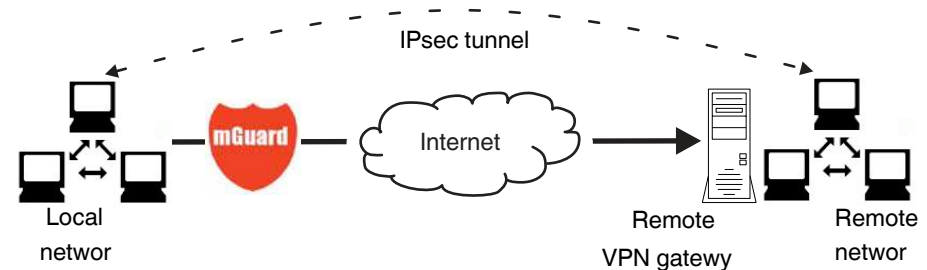
Tunnel settings IPsec/L2TP

If clients should connect via the FL MGUARD by IPsec/L2TP, activate the L2TP server and make the following entries in the fields specified below:

– **Type**: Transport
– **Protocol**: UDP
– **Local Port:** %all
– **Remote Port:** %all

Specifying a default route over the VPN:

Address 0.0.0.0/0 specifies a *default route over the VPN*.

In this case, all data traffic where no other tunnel or route exists is routed through this VPN tunnel.

A default route over the VPN should only be specified for a single tunnel.

	In *Stealth* mode, a *default route over the VPN* cannot be used.

Option following installation of a VPN tunnel group license

If *Address of the remote site's VPN gateway* is specified as **%any**, it is possible that there are many FL MGUARD devices or many networks on the remote side.

A very large address area is then specified in the **Remote** field for the local FL MGUARD. A part of this address area is used on the remote FL MGUARD devices for the network specified for each of them under **Local**.

This is illustrated as follows: The entries in the *Local* and *Remote* fields for the local and remote FL MGUARD devices could be made as follows:

Local FL MGUARD			Remote FL MGUARD **A**	
Local	Remote		Local	Remote
10.0.0.0/8	10.0.0.0/8	>	10.1.7.0/24	10.0.0.0/8
			Remote FL MGUARD **B**	
			Local	Remote
		>	10.3.9.0/24	10.0.0.0/8
			Etc.	

In this way, by configuring a single tunnel, you can establish connections for a number of peers.

ℹ To use this option, the *VPN tunnel group license* must be installed first, unless the device was delivered accordingly. The device must be restarted in order to use this installed license.

Virtual IP address *(only in Stealth mode)*

Figure 5-4   Virtual IP

In *Stealth* mode, the local network of the VPN is simulated by the FL MGUARD. Within this *virtual* network, the client is known as and can be addressed by the *virtual* IP address to be entered here.

IPsec VPN >> Connections >> Edit >> General
Further settings can be made by clicking on **More...**

Options	
Tunnel connection type	

Enabled	**Yes/No**
	As above.
Comment	Freely selectable comment text. Can be left empty.
Type	**Tunnel/Transport**
	As above. When you switch to *Transport*, the following fields (apart from *Protocol)* are hidden as these parameters are omitted.
Local	See "Local" on page 228
Remote	See "Remote" on page 228
Virtual IP for the client	See "Virtual IP for the client" on page 231

Local NAT	**NAT**
	With NAT (**N**etwork **A**ddress **T**ranslation), addresses in data packets are replaced by other addresses.
	It is possible to translate the IP addresses of devices located at the local end of the VPN tunnel (local NAT) or the addresses of devices located at the remote end (remote NAT).

IPsec VPN >> Connections >> Edit >> General [...]		
Further settings can be made by clicking on **More...**		
	Local NAT for IPsec tunnel connections	**Off/1:1 NAT/Local masquerading** Default: **Off** Here you can define which type of address translation is to be used for the destination address of the packets being received and for the source address of the packets being transmitted. **Off**: NAT is not performed. **1:1 NAT** **Local NAT** | Local NAT for IPsec tunnel connections	1:1 NAT ▼
Internal network address for local 1-to-1 NAT	192.168.2.1	 With 1:1 NAT, the IP addresses of devices at the local end of the tunnel are exchanged so that each individual address is translated into another specific address. It is not translated into an address that is identical for all devices (as is the case with IP masquerading). If local devices transmit data packets, only those data packets are considered which: – Are actually encrypted by the FL MGUARD (the FL MGUARD only forwards packets via the VPN tunnel if they originate from a trustworthy source). – Originate from a source address within the network which is defined in conjunction with the subnet mask under *Local* under **Internal network address for local 1-to-1 NAT**. – Have their destination address in the *Remote* network (see "Remote" on page 228) if 1:1 NAT is not set for remote NAT. – Have their destination address in the area corresponding to the *Network address for remote 1-to-1 NAT* if 1:1 NAT is set for remote NAT. The data packets of local devices are assigned a source address according to the address set under *Local* (see "Local" on page 228) and are transmitted via the VPN tunnel.
	Internal network address for local 1-to-1 NAT	Data packets received via the VPN tunnel are assigned the other way around. Destination addresses that belong to the *Local* network are translated into the corresponding address under **Internal networkaddress for local 1-to-1 NAT**.

IPsec VPN >> Connections >> Edit >> General [...]

Further settings can be made by clicking on **More...**

	Local NAT for IPsec tunnel connections	**Local masquerading**

Local NAT

| Local NAT for IPsec tunnel connections | Local masquerading ▼ |
| Internal network address for local masquerading | 192.168.1.0/24 |

If local devices transmit data packets, only those data packets are considered which:

– Are actually encrypted by the FL MGUARD (the FL MGUARD only forwards packets via the VPN tunnel if they originate from a trustworthy source).

– Originate from a source address within the network which is defined under Internal network address for local masquerading.

– Have their destination address in the *Remote* network (see "Remote" on page 228) if 1:1 NAT is not set for remote NAT.

– Have their destination address in the area corresponding to the *Network address for remote 1-to-1 NAT* if 1:1 NAT is set for remote NAT.

The source address of such data packets is masked under *Local* using the lowest IP address of the network. The data packets are then transmitted via the VPN tunnel. Masking changes the source address (and source port). The original addresses are recorded in an entry in the Conntrack table.

Where response packets are received via the VPN tunnel and there is a matching entry in the Conntrack table, these packets have their destination address (and destination port) written back to them. |
| **Remote NAT** | **Remote NAT for IPsec tunnel connections** | **Off/1:1 NAT/Masquerading of remote network**

Here you can define which type of address translation is to be used for the source address of the packets being received and for the destination address of the packets being transmitted.

Default: **Off**

Off: NAT is not performed. |

IPsec VPN >> Connections >> Edit >> General [...]		
Further settings can be made by clicking on **More...**		
Remote NAT	**Remote NAT for IPsec tunnel connections**	**1:1 NAT** Remote NAT Remote NAT for IPsec tunnel connections: 1:1 NAT Network address for remote 1-to-1 NAT: 192.168.2.1 With 1:1 NAT, the IP addresses of the remote devices are exchanged so that each individual address is swapped for another specific address, and is not swapped for an address that is identical for all devices (as is the case with IP masquerading). If local devices transmit data packets, only those data packets are considered which: – Are actually encrypted by the FL MGUARD (the FL MGUARD only forwards packets via the VPN tunnel if they originate from a trustworthy source). – Have their source address within the network defined under *Local NAT* (under *"Local" on page 228,* under *1:1 NAT* or under *Local masquerading)*, or have their source address within the Local network if *Local NAT* is not defined. – Have a destination address which belongs to the **Network address for remote 1-to-1 NAT** if the "Remote" network subnet mask is applied to it. The data packets are assigned a corresponding destination address from the network that is set under **Remote** (see "Remote" on page 228). If necessary, the source address is also replaced (see *Local NAT*). The data packets are then transmitted via the VPN tunnel.
	Network address for remote 1-to-1 NAT	The source addresses of packets received by the FL MGUARD via the VPN tunnel are translated the other way around. These packets arrive with a source address from the network defined under *Remote*. This address is translated using the **Network address for remote 1-to-1 NAT**.
Remote NAT	**Remote NAT for IPsec tunnel connections**	**Masquerading of the remote network** Remote NAT Remote NAT for IPsec tunnel connections: Masquerading of remote net Internal IP address used for remote masquerading: 192.168.1.1 The source addresses of data packets received by the FL MGUARD via the VPN tunnel are masked using the IP address defined under **Internal IP address used for remote masquerding**. The original and translated source address (and source port) are recorded. This means that responses can have their original destination restored if a matching record is found for them. If necessary, the destination address is also translated (see *Local NAT*).

IPsec VPN >> Connections >> Edit >> General [...]		
Further settings can be made by clicking on **More...**		
Protocol	**Protocol**	All/TCP/UDP/ICMP
		Select whether the VPN is restricted to a specific protocol or whether it is valid for all data traffic.
		When TCP or UDP is selected:
		Protocol
		Protocol TCP ▼
		Local Port ("%all' for all ports, a number between 1 and 65535 or '%any' to accept any proposal.) %all
		Remote Port ("%all' for all ports, a number between 1 and 65535 or '%any' to accept any proposal.) %all
	Local Port	**%all** (default) specifies that all ports can be used. If a specific port should be used, specify the port number. **%any** specifies that port selection is made by the client.
	Remote Port	**%all** (default) specifies that all ports can be used. If a specific port should be used, specify the port number.

Local masquerading

> **i**   Can only be used for *Tunnel* VPN type.

Example

A control center has one VPN tunnel each for a large number of branches. One local network with numerous computers is installed in each of the branches, and these computers are connected to the control center via the relevant VPN tunnel. In this case, the address area could be too small to include all the computers at the various VPN tunnel ends.

Local masquerading provides the solution:

The computers connected in the network of a branch appear under a single IP address by means of local masquerading for the VPN gateway of the control center. In addition, this enables the local networks in the various branches to all use the same network address locally. Only the branch can establish VPN connections to the control center.

Internal network address for local masquerading

Specifies the network, i.e., the IP address area, for which local masquerading is used.

The sender address in the data packets sent by a computer via the VPN connection is only replaced by the address specified in the **Local** field (see above) if this computer has an IP address from this address area.

The address specified in the **Local** field must have the subnet mask "/32" to ensure that only one IP address is signified.

> **i**   Local masquerading can be used in the following network modes: Router, PPPoE, PPTP, Modem, Built-in Modem, and Stealth (only "multiple clients" in Stealth mode).
>
> *Modem/Built-in Modem* is not available for all FL MGUARD models (see "Network >> Interfaces" on page 104).

ℹ️ For IP connections via a VPN connection with active local masquerading, the firewall rules for outgoing data in the VPN connection are used for the original source address of the connection.

1:1 NAT

ℹ️ Only in Router mode.

With 1:1 NAT, it is still possible to enter the network addresses actually used (local and/or remote) to specify the tunnel beginning and end, independently of the tunnel parameters agreed with the remote peer:
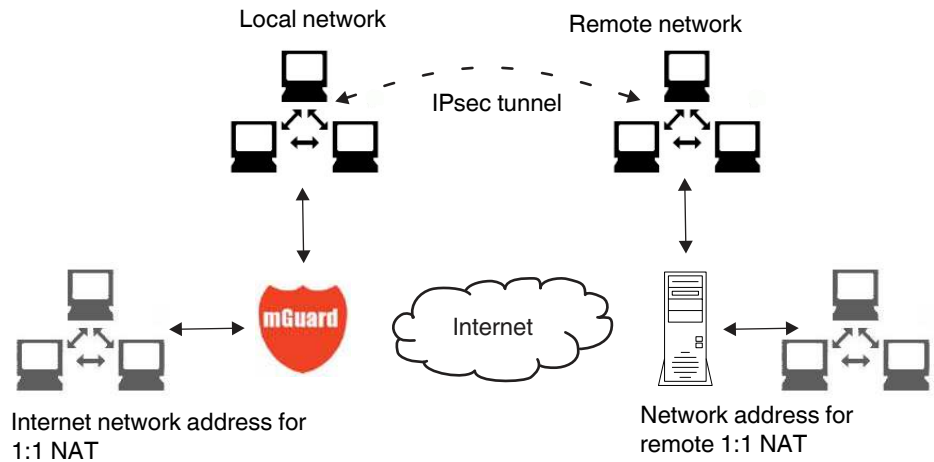
Figure 5-5   1:1 NAT

5.7.2.3 Authentication

IPsec VPN >> Connections >> Edit >> Authentication		
Authentication	Authentication method	There are two options: – X.509 Certificate (default) – Pre-Shared Key (PSK) Depending on the chosen method, the page contains different setting options. **Authentication method: X.509 Certificate** This method is supported by most modern IPsec implementations. With this option, each VPN device has a secret private key and a public key in the form of an X.509 certificate, which contains further information about the certificate's owner and the certification authority (CA). The following must be specified: – How the FL MGUARD authenticates itself to the partner – How the FL MGUARD authenticates the remote partner **How the FL MGUARD authenticates itself to the partner**

IPsec VPN >> Connections >> Edit >> Authentication

	Local X.509 Certificate	Specifies which machine certificate the FL MGUARD uses as authentication to the VPN partner.
		Select one of the machine certificates from the selection list.
		The selection list contains the machine certificates that have been loaded on the FL MGUARD under the *Authentication >> Certificates* menu item (see Page 163).

> **i** If *None* is displayed, a certificate must be installed first. *None* must not be left in place, as this results in no X.509 authentication.

How the FL MGUARD authenticates the remote partner

The following definition relates to how the FL MGUARD verifies the authenticity of the VPN remote partner.

The table below shows which certificates must be provided for the FL MGUARD to authenticate the VPN partner if the VPN partner shows one of the following certificate types when a connection is established:

– A machine certificate signed by a CA

– A self-signed machine certificate

For additional information about the table, see "Authentication >> Certificates" on page 163.

Authentication for VPN

The partner shows the following:	Machine certificate, **signed by CA**	Machine certificate, **self-signed**
The FL MGUARD authenticates the partner using:	⇕	⇕
	Remote certificate Or all CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner	Remote certificate

According to this table, the certificates that must be provided are the ones the FL MGUARD uses to authenticate the relevant VPN partner.

Requirement The following instructions assume that the certificates have already been correctly installed on the FL MGUARD (see "Authentication >> Certificates" on page 163, apart from the remote certificate).

> **i** If the use of revocation lists (CRL checking) is activated under the *Authentication >> Certificates , Certificate settings* menu item, each certificate signed by a CA that is "shown" by the VPN partner must be checked for revocations. This excludes locally configured (imported) remote certificates.

Remote CA Certificate

Self-signed machine certificate

If the VPN partner authenticates itself with a **self-signed** machine certificate:

• Select the following entry from the selection list:

"No CA certificate, but the Remote Certificate below"

• Install the remote certificate under *Remote Certificate* (see "Installing the remote certificate" on page 239).

> **i** It is not possible to reference a remote certificate loaded under the *Authentication >> Certificates* menu item.

Machine certificate signed by the CA

If the VPN partner authenticates itself with a machine certificate **signed by a CA**:

It is possible to authenticate the machine certificate shown by the partner as follows:

– Using CA certificates

– Using the corresponding remote certificate

Authentication using a CA certificate:

Only the CA certificate from the CA that signed the certificate shown by the VPN partner should be referenced here (selection from list). The additional CA certificates that form the chain to the root CA certificate together with the certificate shown by the partner must be installed on the FL MGUARD under the *Authentication >> Certificates* menu item.

The selection list contains all the CA certificates that have been loaded on the FL MGUARD under the *Authentication >> Certificates* menu item.

The other option is "*Signed by any trusted CA*".

With this setting, all VPN partners are accepted, providing that they log in with a signed CA certificate issued by a recognized certification authority (CA). The CA is recognized if the relevant CA certificate and all other CA certificates have been loaded on the FL MGUARD. These then form the chain to the root certificate together with the certificates shown.

Authentication using the corresponding remote certificate:

• Select the following entry from the selection list:

"No CA certificate, but the Remote Certificate below"

• Install the remote certificate under *Remote Certificate* (see "Installing the remote certificate" on page 239).

> **i** It is not possible to reference a remote certificate loaded under the *Authentication >> Certificates* menu item.

Installing the remote certificate

The remote certificate must be configured if the VPN partner is to be authenticated using a remote certificate.

To import a certificate, proceed as follows:

Requirement	The certificate file (file name extension: *.pem, *.cer or *.crt) is saved on the connected computer.
	• Click on **Browse...** to select the file.
	• Click on **Upload**.
	The contents of the certificate file are then displayed.

IPsec VPN >> Connections >> Edit >> Authentication		
VPN Identifier	**Authentication method: CA certificate**	
	The following explanation applies if the VPN partner is authenticated using CA certificates.	
	VPN gateways use the VPN identifier to detect which configurations belong to the same VPN connection.	
	If the FL MGUARD consults CA certificates to authenticate a VPN partner, then it is possible to use the VPN identifier as a filter.	
	• Make a corresponding entry in the *Remote* field.	
	Local	Default: empty field
		The local VPN identifier can be used to specify the name the FL MGUARD uses to identify itself to the partner. It must match the data in the machine certificate of the FL MGUARD.
		Valid values:
		– Empty, i.e., no entry (default). The "Subject" entry (previously *Distinguished Name*) in the machine certificate is then used.
		– The "Subject" entry in the machine certificate.
		– One of the *Subject Alternative Names*, if they are listed in the certificate. If the certificate contains *Subject Alternative Names*, these are specified under "Valid values". These can include IP addresses, host names with "@" prefix or e-mail addresses.
	Remote	Specifies what must be entered as a subject in the machine certificate of the VPN partner for the FL MGUARD to accept this VPN partner as a communication partner.
		It is then possible to limit or enable access by VPN partners, which the FL MGUARD would accept in principle based on certificate checks:
		– Limited access to certain *subjects* (i.e., machines) and/or to *subjects* that have certain attributes
		– Access enabled for all *subjects*
		i "Distinguished Name" was previously used instead of "Subject".

IPsec VPN >> Connections >> Edit >> Authentication [...]

Access enabled for all subjects:

If the *Remote* field is left empty, then any subject entries are permitted in the machine certificate shown by the VPN partner. It is then no longer necessary to identify or define the subject in the certificate.

Limited access to certain subjects:

In the certificate, the certificate owner is specified in the *Subject* field. The entry is comprised of several attributes. These attributes are either expressed as an object identifier (e.g., 132.3.7.32.1) or, more commonly, as an abbreviation with a corresponding value.

Example: CN=VPN endpoint 01, O=Smith and Co., C=US

If certain subject attributes have very specific values for the acceptance of the VPN partner by the FL MGUARD, then these must be specified accordingly. The values of the other freely selectable attributes are entered using the * (asterisk) wildcard.

Example: CN=*, O=Smith and Co., C=US (with or without spaces between attributes)

In this example, the attributes "O=Smith and Co." and "C=US" should be entered in the certificate that is shown under "Subject". It is only then that the FL MGUARD would accept the certificate owner (subject) as a communication partner. The other attributes in the certificates to be filtered can have any value.

i	Please note the following when setting a subject filter:
	The number and the order of the attributes must correspond to that of the certificates for which the filter is to be used
	Please note these are case-sensitive.

IPsec VPN >> Connections >> Edit >> Authentication [...]	
VPN Identifier	**Authentication method: Pre-Shared Secret (PSK)** IPsec VPN » Connections » Mannheim-Leipzig General **Authentication** Firewall IKE Options **Authentication** Authentication method Pre-Shared Secret (PSK) ▼ Pre-Shared Secret Key (PSK) complicated_like_5Dy0qoD_and_long **VPN Identifier** Local By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname"). Remote By default the IP address of the peer is used. Other possible settings are a hostname ("@hostname") or an e-mail address ("name@hostname"). This method is mainly supported by older IPsec implementations. In this case, both sides of the VPN authenticate themselves using the same PSK. To make the agreed key available to the FL MGUARD, proceed as follows: • Enter the agreed string in the **Pre-Shared Secret Key (PSK)** entry field. ℹ️ To achieve security comparable to that of 3DES, the string should consist of around 30 randomly selected characters, and should include upper and lower case characters and digits. ℹ️ *Pre-Shared Secret Key* cannot be used with dynamic (%any) IP addresses. Only fixed IP addresses or host names on both sides are supported. However, changing IP addresses (DynDNS) can be hidden behind the host name. ℹ️ *Pre-Shared Secret Key* cannot be used if at least one (or both) of the communication partners is located downstream of a NAT gateway. VPN gateways use the *VPN Identifier* to detect which configurations belong to the same VPN connection. The following entries are valid for PSK: – Empty (IP address used by default) – An IP address – A host name with "@" prefix (e.g., "@vpn1138.example.com") – An e-mail address (e.g., "piepiorra@example.com")

5.7.2.4 Firewall

Incoming/Outgoing

While the settings made under the *Network Security* menu item only relate to non-VPN connections (see above under "Network Security menu" on page 179), the settings here only relate to the VPN connection defined on these tab pages.

If multiple VPN connections have been defined, you can limit the outgoing or incoming access individually for each connection. Any attempts to bypass these restrictions can be logged.

| i | By default, the VPN firewall is set to allow all connections for this VPN connection. However, the extended firewall settings defined and explained above apply independently for each individual VPN connection (see "Network Security menu" on page 179, "Network Security >> Packet Filter" on page 179, "Advanced" on page 188). |

| i | If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored. |

| i | In *Stealth* mode, the actual IP address used by the client should be used in the firewall rules, or it should be left at 0.0.0.0/0, as only one client can be addressed through the tunnel. |

| i | If the *Allow packet forwarding between VPN connections* option is set to **Yes** on the *Global* tab page, the rules under **Incoming** are used for the incoming data packets to the FL MGUARD, and the rules under **Outgoing** are applied to the outgoing data packets. If the outgoing data packets are included in the same connection definition (for a defined VPN connection group), then the firewall rules for **Incoming** and **Outgoing** for the same connection definition are used. If a different VPN connection definition applies to the outgoing data packets, the firewall rules for **Outgoing** for this other connection definition are used. |

> ℹ️ If the FL MGUARD has been configured to forward SSH connection packets (e.g., by permitting a SEC-Stick hub & spoke connection), existing VPN firewall rules are not applied. This means, for example, that packets of an SSH connection are sent via a VPN tunnel despite the fact that this is prohibited by its firewall rules.

IPsec VPN >> Connections >> Edit >> Firewall		
Incoming	**General firewall setting**	**Allow all incoming connections**: The data packets of all incoming connections are allowed.
		Drop all incoming connections: The data packets of all incoming connections are discarded.
		Use the firewall ruleset below: Displays further setting options. (This menu item is not included in the scope of functions for the FL MGUARD RS2000).
	The following settings are only visible if "**Use the firewall ruleset below**" is set.	
	Protocol	**All** means TCP, UDP, ICMP, GRE, and other IP protocols
	From IP/To IP	**0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
		Incoming:
		– From IP: The IP address in the VPN tunnel
		– To IP: The 1:1 NAT address or the actual address
		Outgoing:
		– From IP: The 1:1 NAT address or the actual address
		– To IP: The IP address in the VPN tunnel
	From Port/To Port	(Only evaluated for TCP and UDP protocols.)
		– **any** refers to any port.
		– **startport:endport** (e.g., 110:120) refers to a port area.
		Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	Action	**Accept** means that the data packets may pass through.
		Reject means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, Reject has the same effect as Drop.)
		Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.
	Comment	Freely selectable comment for this rule.
	Log	For each individual firewall rule, you can specify whether the use of the rule:
		– Should be logged – set *Log* to **Yes**
		– Should not be logged – set *Log* to **No** (default settings).

IPsec VPN >> Connections >> Edit >> Firewall

	Log entries for unknown connection attempts	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged.
Outgoing		The explanation provided under "Incoming" also applies to "Outgoing".

5.7.2.5   IKE Options

IPsec VPN >> Connections >> Edit >> IKE Options		
ISAKMP SA (Key Exchange)	**Algorithms**	ℹ️ Decide on which encryption method should be used with the administrator of the partner.
		Encryption
		3DES-168 is the most commonly used method and is therefore set by default.
		Fundamentally, the following applies: the more bits an encryption algorithm has (specified by the appended number), the more secure it is. The relatively new AES-256 method is therefore the most secure, however it is still not used that widely.
		The longer the key, the more time-consuming the encryption procedure. However, this does not affect the FL MGUARD as it uses a hardware-based encryption technique. Nevertheless, this aspect may be of significance for the partner.
		The algorithm designated as "Null" does not contain encryption.
		Hash
		Leave this set to *All algorithms*. It then does not matter whether the partner is operating with MD5, SHA-1, SHA-256, SHA-384 or SHA-512.
		The encryption algorithms SHA-256 and SHA-512 are supported by all FL MGUARD devices. However, not all FL MGUARD devices accelerate the algorithms via hardware.
		On the other FL MGUARD devices, MD5 and SHA1 are accelerated with hardware. Only the FL MGUARD SMART2 also accelerates SHA-256 via hardware.
IPsec SA (Data Exchange)	In contrast to *ISAKMP SA (key exchange)* (see above), the procedure for data exchange is defined here. It does not necessarily have to differ from the procedure defined for key exchange.	
	Algorithms	See above.

IPsec VPN >> Connections >> Edit >> IKE Options		
	Perfect Forward Secrecy (PFS)	Method for providing increased security during data transmission. With IPsec, the keys for data exchange are renewed at defined intervals.
		With PFS, new random numbers are negotiated with the partner instead of being derived from previously agreed random numbers.
		The partner must have the same entry. We recommend activation for security reasons.
		$\mathbf{i}$ Select **Yes**, if the partner supports PFS.
		$\mathbf{i}$ Set *Perfect Forward Secrecy (PFS)* to **No** if the partner is an IPsec/L2TP client.
Lifetimes and Limits	**The keys of an IPsec connection are renewed at defined intervals in order to increase the difficulty of an attack on an IPsec connection.**	
	ISAKMP SA Lifetime	Lifetime in seconds of the keys agreed for ISAKMP SA. Default setting: 3600 seconds (1 hour). The maximum permitted lifetime is 86400 seconds (24 hours).
	IPsec SA Lifetime	Lifetime in seconds of the keys agreed for IPsec SA.
		Default setting: 28800 seconds (8 hours). The maximum permitted lifetime is 86400 seconds (24 hours).
	IPsec SA Traffic Limit	0 to 2147483647 bytes
		The value 0 indicates that there is no traffic limit for the IPsec SAs on this VPN connection.
		All other values indicate the maximum number of bytes which are encrypted by the IPsec SA for this VPN connection (Hard Limit).
	Re-key Margin for Lifetimes	Applies to ISAKMP SAs and IPsec SAs.
		Minimum duration before the old key expires and during which a new key should be created. Default setting: 540 seconds (9 minutes).

IPsec VPN >> Connections >> Edit >> IKE Options		
	Re-key Margin for the Traffic Limit	Only applies to IPsec SAs.
		The value 0 indicates that the traffic limit is not used.
		0 must be set here when 0 is also set under *IPsec SA Traffic Limit*.
		If a value above 0 is entered, then a new limit is calculated from two values. The number of bytes entered here is subtracted from the value specified under *IPsec SA Traffic Limit* (i.e. *Hard Limit*).
		The calculated value is then known as the *Soft Limit*. This specifies the number of bytes which must be encrypted for a new key to be negotiated for the IPsec SA.
		A further amount is subtracted when a Re-key Fuzz (see below) above 0 is entered. This is a percentage of the re-key margin. The percentage is entered under Re-key Fuzz.
		The re-key margin value must be lower than the *Hard Limit*. It must be significantly lower when a *Re-key Fuzz* is also added.
		If the *IPsec SA Lifetime* is reached earlier, the *Soft Limit* is ignored.
	Re-key Fuzz	Maximum percentage by which *Re-key Margin* is to be increased at random. This is used to delay key exchange on machines with multiple VPN connections. Default setting: 100 percent
	Keying tries	Number of attempts to negotiate new keys with the partner.
		The value 0 results in unlimited attempts for connections initiated by the FL MGUARD, otherwise it results in 5 attempts.
	Rekey	**Yes/No**
		When set to **Yes**, the FL MGUARD will attempt to negotiate a new key when the old one expires.
Dead Peer Detection		**If the partner supports the Dead Peer Detection (DPD) protocol, the relevant partners can detect whether or not the IPsec connection is still valid and whether it needs to be established again.**
	Delay between requests for a sign of life	Duration in seconds after which *DPD Keep Alive* requests should be transmitted. These requests test whether the partner is still available.
		Default setting: 30 seconds.

IPsec VPN >> Connections >> Edit >> IKE Options		
	Timeout for absent sign of life after which peer is assumed dead	Duration in seconds after which the connection to the partner should be declared dead if there has been no response to the *Keep Alive* requests. Default setting: 120 seconds. If the FL MGUARD finds that a connection is dead, it responds according to the setting under **Connection startup** (see definition of this VPN connection under **Connection startup** on the *General* tab page).

5.7.3   IPsec VPN >> L2TP over IPsec

> **i** These settings are not applied in Stealth mode.

Allows VPN connections to the FL MGUARD to be established using the IPsec/L2TP protocol.

In doing so, the L2TP protocol is driven using an IPsec transport connection in order to establish a tunnel connection to a Point-to-Point Protocol (PPP). Clients are automatically assigned IP addresses by the PPP.

In order to use IPsec/L2TP, the L2TP server must be activated and one or more IPsec connections with the following properties must be defined:

– Type: Transport
– Protocol: UDP
– Local Port: %all
– Remote Port: %all
– PFS: No

(See also "Further settings can be made by clicking on **More...**" on page 5-231 and "IKE Options" on page 246.)

5.7.3.1   L2TP Server

```
IPsec VPN » L2TP over IPsec

  L2TP Server

  Settings

  Start L2TP Server for      No  ▼
  IPsec/L2TP?

  Local IP for L2TP connections    10.106.106.1

  Remote IP range start    10.106.106.2

  Remote IP range end    10.106.106.254

  Please note: These settings don't apply to the Stealth mode.

  Status

  The L2TP daemon isn't running.
```

IPsec VPN >> L2TP over IPsec >> L2TP Server		
Settings	Start L2TP Server for IPsec/L2TP?	If you want to enable IPsec/L2TP connections, set this option to **Yes**.
		It is then possible to establish L2TP connections to the FL MGUARD via IPsec, which dynamically assign IP addresses to the clients within the VPN.
	Local IP for L2TP connections	If set as shown in the screenshot above, the FL MGUARD will inform the partner that its address is 10.106.106.1.
	Remote IP range start/end	If set as shown in the screenshot above, the FL MGUARD will assign the partner an IP address between 10.106.106.2 and 10.106.106.254.
	Status	Displays information about the L2TP status if this connection type has been selected.

5.7.4   IPsec VPN >> IPsec Status

Displays information about the status of IPsec connections.

The names of the VPN connections are listed on the left, while their current status is indicated on the right.

Buttons

Update   To update the displayed data, if necessary, click on **Update**.

Restart   If you want to disconnect and then restart a connection, click on the corresponding **Restart** button.

Edit   If you want to reconfigure a connection, click on the corresponding **Edit** button.

Connection, ISAKAMP State, IPsec State

Gateway   *Gateway* indicates the IP addresses of the communicating VPN gateways.

Traffic   *Traffic* refers to the computers and networks that communicate via the VPN gateways.

ID   Refers to the subject of an X.509 certificate.

ISAKMP State   *ISAKMP State* (Internet Security Association and Key Management Protocol) is set to "established" if both VPN gateways involved have established a channel for key exchange. In this case, they have been able to contact one another and all entries up to and including "ISAKMP SA" on the connection configuration page are correct.

IPsec State   *IPsec State* is set to "established" if IPsec encryption is activated for communication. In this case, the data under "IPsec SA" and "Tunnel Settings" is also correct.

In the event of problems, it is recommended that you check the VPN logs of the partner to which the connection was established. This is because detailed error messages are not forwarded to the initiating computer for security reasons.

If displayed:	This means that:
ISAKMP SA established, IPsec State: WAITING	Authentication was successful, but the other parameters did not match. Does the connection type (tunnel, transport) correspond? If "Tunnel" is selected, do the network areas match on both sides?
IPsec State: IPsec SA established	The VPN connection is established successfully and can be used. However, if this is not possible, the VPN gateway of the partner is causing problems. In this case, deactivate and reactivate the connection to reestablish the connection.

5.8   SEC-Stick menu

The FL MGUARD supports the use of an SEC-Stick, which is an access protector for IT systems. The SEC-Stick is a product of the team2work company: www.team2work.de

The SEC-Stick is a key. It can be inserted into the USB port of a computer with an Internet connection, and can then set up an encrypted connection to the FL MGUARD in order to securely access defined services in the office or home network. The Remote Desktop Protocol, for example, can be used within the encrypted and secure SEC-Stick connection to control a PC remotely in the office or at home, as if the user was sitting directly in front of it.

In order for this to work access to the business PC is protected by the FL MGUARD and the FL MGUARD must be configured for the SEC-Stick to permit access because the user of this remote computer, into which the SEC-Stick is inserted, authenticates herself/himself to the FL MGUARD using the data and software stored on her/his SEC-Stick.

The SEC-Stick establishes an SSH connection to the FL MGUARD. Additional channels can be embedded into this connection, e.g., TCP/IP connections.

5.8.1   Global

SEC-Stick >> Global >> Access

SEC-Stick Access

This menu item is not included in the scope of functions for the FL MGUARD RS2000.

Access via the SEC-Stick requires a license. This access function can only be used if the corresponding license has been purchased and installed.

SEC-Stick >> Global >> Access [...]		
	Enable SEC-Stick service	Set this option to **Yes** to specify that the SEC-Stick being used at a remote location or its owner is able to log in. In this case, SEC-Stick remote access must also be enabled (next option).
	Enable SEC-Stick remote access	Set this option to **Yes** to enable SEC-Stick remote access.
	Remote SEC-Stick TCP Port	Default: 22002
		If this port number is changed, the new port number only applies for access via the *External, External 2* or *VPN* interface. Port number 22002 still applies for internal access.
	Delay between requests for a sign of life	Default: 120 seconds
		Values from 0 to 3600 seconds can be set. Positive values indicate that the FL MGUARD is sending a query to the partner within the encrypted SSH connection to find out whether it can still be accessed. The request is sent if no activity was detected from the partner for the specified number of seconds (e.g., due to network traffic within the encrypted connection).
		The value entered relates to the functionality of the encrypted SSH connection. As long as the functions are working properly, the SSH connection is not terminated by the FL MGUARD as a result of this setting, even when the user does not perform any actions during this time.
		Because the number of simultaneously open sessions is limited (see *Maximum number of cumulative concurrent sessions for all users*), it is important to terminate sessions that have expired.
		Therefore, the request for a sign of life is preset to 120 seconds in the case of Version 7.4.0 or later. If a maximum of three requests for a sign of life are issued, this causes an expired session to be detected and removed after six minutes.
		In previous versions, the preset was "0". This means that no requests for a sign of life are sent.
		Please note that sign of life requests generate additional traffic.
	Maximum number of missing signs of life	Specifies the maximum number of times a sign of life request to the partner may remain unanswered. For example, if a sign of life request should be made every 15 seconds and this value is set to 3, then the SEC-Stick client connection is deleted if a sign of life is not detected after approximately 45 seconds.
Concurrent Session Limits	The number of simultaneous sessions is limited for SEC-Stick connections. Approximately 0.5 Mbytes of memory space is required for each session to ensure the maximum level of security.	
	The restriction does not affect existing sessions; it only affects newly established connections.	

SEC-Stick >> Global >> Access [...]

	Maximum number of cumulative concurrent sessions for all users	0 to 2147483647
		Specifies the number of connections that are permitted for all users simultaneously. When "0" is set, no session is permitted.
	Maximum number of concurrent sessions for one user	0 to 2147483647
		Specifies the number of connections that are permitted for one user simultaneously. When "0" is set, no session is permitted.

Allowed Networks **Lists the firewall rules that have been set up for SEC-Stick remote access.**

N°	From IP	Interface	Action	Comment	Log
	0.0.0.0/0	External ▼	Accept ▼		No ▼

If multiple firewall rules are defined, these are queried starting from the top of the list of entries until an appropriate rule is found. This rule is then applied. If the list of rules contains further subsequent rules that could also apply, these rules are ignored.

The rules specified here only take effect if **Enable SEC-Stick remote access** is set to **Yes**. *Internal* access is also possible when this option is set to *No*. A firewall rule that would refuse *Internal* access does therefore not apply in this case.

Multiple rules can be specified.

From IP Enter the address of the computer/network from which remote access is permitted or forbidden in this field.

IP address **0.0.0.0/0** means all addresses. To specify an address area, use CIDR format (see 5-294).

Interface **External/Internal/External 2/VPN/Dial-in[1]**

Specifies to which interface the rule should apply.

If no rules are set or if no rule applies, the following default settings apply:
– Remote SEC-Stick access is permitted via *Internal, VPN*, and *Dial-in*.
– Access via *External* and *External 2* is refused.

Specify the access options according to your requirements.

> **i** If you want to refuse access via *Internal, VPN* or *Dial-in*, you must implement this explicitly by means of corresponding firewall rules, for example, by specifying *Drop* as an action.

Action **Accept** means that the data packets may pass through.

Reject means that the data packets are sent back and the sender is informed of their rejection. (In *Stealth* mode, *Reject* has the same effect as *Drop*.)

Drop means that the data packets are not permitted to pass through. They are discarded, which means that the sender is not informed of their whereabouts.

Comment Freely selectable comment for this rule.

SEC-Stick >> Global >> Access [...]		
	Log	For each individual firewall rule, you can specify whether the use of the rule: – Should be logged – set *Log* to **Yes** – Should not be logged – set *Log* to **No** (default setting)

¹ *External 2* and *Dial-in* are only for devices with a serial interface (see "Network >> Interfaces" on page 104).

5.8.2   Connections

SEC-Stick >> Connections >> SEC-Stick connections		
SEC-Stick connections	**List of defined SEC-Stick connections. Click on the down arrow at the top left of the screen if you want to add a new connection. An existing connection can be edited by clicking on Edit.**	
	Not all of the SEC-Stick functions can be configured via the web interface of the FL MGUARD.	
	Enabled	To use a defined SEC-Stick connection, the **Enabled** option must be set to **Yes**.
	User Name	An SEC-Stick connection with a uniquely assigned user name must be defined for every owner of a SEC-Stick who has authorized access. This user name is used to uniquely identify the defined connections.
	Name	Name of the person.
	Company	Name of the company.
	The following page appears when you click on **Edit**:	
General	**Enabled**	As above

SEC-Stick >> Connections >> SEC-Stick connections [...]		
	User Name	As above
	Comment	Optional comment text.
	Contact	Optional comment text.
	A descriptive name of the user	Optional name of the person (repeated).
	Company	Optional: As above
	SSH public key (including ssh-dss or ssh-rsa)	Enter the SSH public key belonging to the SEC-Stick in ASCII format in this field. The secret equivalent is stored on the SEC-Stick.
SSH Port Forwarding	**List of allowed access and SSH port forwarding relating to the SEC-Stick of the corresponding user.**	
	IP	IP address of the computer to which access is enabled.
	Port	Port number to be used when accessing the computer.

5.9 QoS menu

$\mathbf{i}$	This menu is **not** available on the **FL MGUARD RS2000**.

QoS (Quality of Service) refers to the quality of individual transmission channels in IP networks. This relates to the allocation of specific resources to specific services or communication types so that they work correctly. The necessary bandwidth, for example, must be provided to transmit audio or video data in realtime in order to reach a satisfactory communication level. At the same time, slower data transfer by FTP or e-mail does not threaten the overall success of the transmission process (file or e-mail transfer).

5.9.1 Ingress Filters

An ingress filter prevents the processing of certain data packets by filtering and dropping them before they enter the FL MGUARD processing mechanism. The FL MGUARD can use an ingress filter to avoid processing data packets that are not needed in the network. This results in a faster processing of the remaining, i.e., required data packets.

Using suitable filter rules, administrative access to the FL MGUARD can be ensured with high probability, for example.

Packet processing on the FL MGUARD is generally defined by the handling of individual data packets. This means that the processing performance depends on the number of packets to be processed and not on the bandwidth.

Filtering is performed exclusively according to features that are present or may be present in each data packet: The sender and recipient IP address specified in the header, the specified Ethernet protocol, the specified IP protocol, the specified TOS/DSCP value and/or the VLAN ID (if VLANs have been set up). As the list of filter rules must be applied to each individual data packet, it should be kept as short as possible. Otherwise, the time spent on filtering could be longer than the time actually saved by setting the filter.

Please note that not all specified filter criteria should be combined. For example, it does not make sense to specify an additional IP protocol in the same rule that contains the ARP Ethernet protocol. Nor does it make sense to specify a transmitter or sender IP address if the IPX Ethernet protocol is specified (in hexadecimal format).

5.9.1.1 Internal/External

Internal: Settings for the ingress filter at the LAN interface

External: Settings for the ingress filter at the WAN interface

QoS >> Ingress Filters >> Internal/External		
Enabling	**Enable Ingress QoS**	**No** (default): This feature is disabled. If filter rules are defined, they are ignored.
		Yes: This feature is enabled. Data packets may only pass through and be forwarded to the FL MGUARD for further evaluation and processing if they comply with the filter rules defined below.
		Filters can be set for the LAN port (**Internal** tab page) and the WAN port (**External** tab page).
	Measurement Unit	**kbit/s or Packet/s**
		Specifies the unit of measurement for the numerical values entered under **Guaranteed** and **Upper Limit**.
Filters	**Use VLAN**	If a VLAN is set up, the relevant VLAN ID can be specified to allow the relevant data packets to pass through. To do this, this option must be set to **Yes**.
	VLAN ID	Specifies that the VLAN data packets that have this VLAN ID may pass through. (To do this, the **Use VLAN** option must be set to **Yes**.)
	Ethernet Protocol	Specifies that only data packets of the specified Ethernet protocol may pass through. Possible entries: **ARP**, **IPV4**, **%any**. Other entries must be in hexadecimal format (up to 4 digits).
		(The ID of the relevant protocol in the Ethernet header is entered here. It can be found in the publication of the relevant standard.)

QoS >> Ingress Filters >> Internal/External [...]		
	IP Protocol	**All/TCP/UDP/ICMP/ESP**
		Specifies that only data packets of the selected IP protocol may pass through. When set to **All**, no filtering is applied according to the IP protocol.
	From IP	Specifies that only data packets from a specified IP address may pass through.
		0.0.0.0/0 stands for all addresses, i.e., in this case no filtering is applied according to the IP address of the sender. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
	To IP	Specifies that only data packets that should be forwarded to the specified IP address may pass through.
		Entries correspond to *From IP*, as described above.
		0.0.0.0/0 stands for all addresses, i.e., in this case no filtering is applied according to the IP address of the sender.
	Current TOS/DSCP	Each data packet contains a TOS or DSCP field. (TOS stands for Type of Service, DSCP stands for Differentiated Services Code Point). The traffic type to which the data packet belongs is specified here. For example, an IP phone will write a different entry in this field for outgoing data packets compared to an FTP program.
		When a value is selected here, only data packets with this value in the TOS or DSCP field may pass through. When set to **All**, no filtering according to the TOS/DSCP value is applied.
	Guaranteed	The number entered specifies how many data packets per second or kbps can pass through at all times – according to the option set under **Measurement Unit** (see above). This applies to the data stream that conforms to the rule set criteria specified on the left (i.e., that may pass through). The FL MGUARD **may** drop the excess number of data packets in the event of capacity bottlenecks if this data stream delivers more data packets per second than specified.
	Upper Limit	The number entered specifies the maximum number of data packets per second or kbps that can pass through – according to the option set under **Measurement Unit** (see above). This applies to the data stream that conforms to the rule set criteria specified on the left (i.e., that may pass through). The FL MGUARD drops the excess number of data packets if this data stream delivers more data packets per second than specified.
	Comment	Optional comment text.

5.9.2   Egress Queues

The services are assigned corresponding priority levels. In the event of connection bottlenecks, the outgoing data packets are placed in egress queues (i.e., queues for pending packets) according to the assigned priority level and are then processed according to their priority. Ideally, the assignment of priority levels and bandwidths should result in a sufficient bandwidth level always being available for the realtime transmission of data packets, while other packets, e.g., FTP downloads, are temporarily set to wait in critical cases.

The main application of egress QoS is the optimal utilization of the available bandwidth on a connection. In certain cases, a limitation of the packet rate can be useful, e.g., to protect a slow computer from overloading in the protected network.

The *Egress Queues* feature can be used for all interfaces and for VPN connections.

5.9.2.1   Internal/External/External 2/Dial-in

Internal: Settings for egress queues on the LAN interface

External: Settings for egress queues on the external WAN interface

External 2: Settings for egress queues on the secondary external interface

QoS » Egress Queues

| Internal | External | External 2 | Dial-in |

Enabling

Enable Egress QoS   No ▼

Total Bandwidth/Rate

Bandwidth/Rate Limit   unlimited   kbit/s ▼

Queues

N°	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High ▼	
2	Important	10	unlimited	Medium ▼	
3	Default	10	unlimited	Medium ▼	
4	Low Priority	10	unlimited	Low ▼	

Dial-in: Settings for egress queues for packets for a PPP dial-up line connection (dial-in)

QoS » Egress Queues

| Internal | External | External 2 | Dial-in |

Enabling

Enable Egress QoS   No ▼

Total Bandwidth/Rate

Bandwidth/Rate Limit   unlimited   kbit/s ▼

Queues

N°	Name	Guaranteed	Upper Limit	Priority	Comment
1	Urgent	10	unlimited	High ▼	
2	Important	10	unlimited	Medium ▼	
3	Default	10	unlimited	Medium ▼	
4	Low Priority	10	unlimited	Low ▼	

5.9.3   Egress Queues (VPN)

5.9.3.1   VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in

VPN via Internal: Settings for egress queues

VPN via External: Settings for egress queues

VPN via External 2: Settings for egress queues

VPN via Dial-in: Settings for egress queues

All of the tab pages listed above for *Egress Queues* for the *Internal, External, External 2,* and *Dial-in* interfaces, and for VPN connections routed via these interfaces, have the same setting options.

In all cases, the settings relate to the data that is sent externally into the network from the relevant FL MGUARD interface.

QoS menu >> Egress Queues >> Internal/External/External 2/Dial-in		
QoS menu >> Egress Queues (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in		
Enabling	**Enable Egress QoS**	**No** (default): This feature is disabled.
		Yes: This feature is enabled. This option is recommended if the interface is connected to a network with low bandwidth. This enables bandwidth allocation to be influenced in favor of particularly important data.
Total Bandwidth/Rate	**Bandwidth/Rate Limit**	**kbit/s or Packet/s**
		Total maximum bandwidth that is physically available – specified in kbps or packets per second.
		In order to optimize prioritization, the total bandwidth specified here should be slightly lower than the actual amount. This prevents a buffer overrun on the transferring devices, which would result in adverse effects.
Queues	**Name**	The default name for the egress queue can be adopted or another can be assigned. The name does not specify the priority level.
	Guaranteed	Bandwidth that should be available at all times for the relevant queue. Based on the selection under **Bandwidth/Rate Limit** (**kbit/s** OR **Packet/s**), meaning that the unit of measurement does not have to be specified explicitly here.
		The total of all guaranteed bandwidths must be less than or equal to the total bandwidth.

QoS menu >> Egress Queues >> Internal/External/External 2/Dial-in		
QoS menu >> Egress Queues (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in [...]		
	Upper Limit	Maximum bandwidth available that may be set for the relevant queue by the system. Based on the selection under **Bandwidth/Rate Limit** (**kbit/s** OR **Packet/s**), meaning that the unit of measurement does not have to be specified explicitly here.
		The value must be greater than or equal to the guaranteed bandwidth. The value **unlimited** can also be specified, which means that there is no further restriction.
	Priority	**Low/Medium/High**
		Specifies with which priority the affected queue should be processed, providing the total available bandwidth has not been exhausted.
	Comment	Optional comment text.

5.9.4 Egress Rules

This page defines the rules for the data that is assigned to the defined egress queues (see above) in order for the data to be transmitted with the priority assigned to the relevant queue.

Rules can be defined separately for all interfaces and for VPN connections.

5.9.4.1 Internal/External/External 2/Dial-in

Internal: Settings for egress queue rules

N°	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

External: Settings for egress queue rules

N°	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

External 2: Settings for egress queue rules

N°	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

Dial-in: Settings for egress queue rules

N°	Protocol	From IP	From Port	To IP	To Port	Current TOS/DSCP	New TOS/DSCP	Queue Name	Comment
1	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Delay	Unchanged	Urgent	
2	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Maximize Reliability	Unchanged	Important	
3	All	0.0.0.0/0	any	0.0.0.0/0	any	TOS: Minimize Cost	Unchanged	Low Priority	

5.9.4.2 Egress Rules (VPN)

VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in

VPN via Internal: Settings for egress queue rules

VPN via External: Settings for egress queue rules

VPN via External 2: Settings for egress queue rules

VPN via Dial-in: Settings for egress queue rules

All of the tab pages listed above for *Egress Rules* for the *Internal, External, External 2,* and *Dial-in* interfaces, and for VPN connections routed via these interfaces, have the same setting options.

In all cases, the settings relate to the data that is sent externally into the network from the relevant FL MGUARD interface.

QoS menu >> Egress Rules >> Internal/External/External 2/Dial-in		
QoS menu >> Egress Rules (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in		
Default	**Default Queue**	*Name of the egress queue* (user-defined).
		The names of the queues are displayed as listed or specified under *Egress Queues* on the *Internal*/*External*/*VPN via External* tab pages. The following default names are defined: Default/Urgent/Important/Low Priority.
		Traffic that is **not** assigned to a specific egress queue under *Rules* remains in the *default queue*. You can specify which egress queue should be used as the *default queue* in this selection list.
	Rules	The assignment of specific data traffic to an egress queue is based on a list of criteria. If the criteria in a row apply to a data packet, it is assigned to the egress queue specified in the row.
		Example: For audio data to be transmitted, you have defined a queue with guaranteed bandwidth and priority under Egress Queues (see Page 261) under the name *Urgent*. You then define the rules here for how audio data is detected and specify that this data should belong to the *Urgent* queue.
	Protocol	**All/TCP/UDP/ICMP/ESP**
		Protocol(s) relating to the rule.
	From IP	IP address of the network or device from which the data originates.
		0.0.0.0/0 means all IP addresses. To specify an address area, use CIDR format (see "CIDR (Classless Inter-Domain Routing)" on page 294).
		Assign the traffic from this source to the queue selected under *Queue Name* in this row.
	From Port	Port used at the source from which data originates (only evaluated for TCP and UDP protocols).
		– **any** refers to any port.
		– **startport:endport** (e.g., 110:120) refers to a port area.
		Individual ports can be specified using the port number or the corresponding service name (e.g., 110 for pop3 or pop3 for 110).
	To IP	IP address of the network or device to which the data is sent. Entries correspond to *From IP*, as described above.
	To Port	Port used at the source where the data is sent. Entries correspond to *From Port*, as described above.

QoS menu >> Egress Rules >> Internal/External/External 2/Dial-in		
QoS menu >> Egress Rules (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in [...]		
	Current TOS/DSCP	Each data packet contains a TOS or DSCP field. (TOS stands for Type of Service, DSCP stands for Differentiated Services Code Point). The traffic type to which the data packet belongs is specified here. For example, an IP phone will write a different entry in this field for outgoing data packets compared to an FTP program that uploads data packet to a server.
		When you select a value here, only the data packets that have this TOS or DSCP value in the corresponding fields are chosen. These values are then set to a different value according to the entry in the **New TOS/DSCP** field.
	New TOS/DSCP	If you want to change the TOS/DSCP values of the data packets that are selected using the defined rules, enter the text that should be written in the TOS/DSCP field here.
		For a more detailed explanation of the **Current TOS/DSCP** and **New TOS/DSCP** options, please refer to the following RFC documents:
		– RFC 3260 "New Terminology and Clarifications for Diffserv"
		– RFC 3168 "The Addition of Explicit Congestion Notification (ECN) to IP"
		– RFC 2474 "Definition of the Differentiated Services Field (DS Field)"
		– RFC 1349 "Type of Service in the Internet Protocol Suite"
	Queue Name	Name of the egress queue to which traffic should be assigned.
	Comment	Optional comment text.

5.10   Redundancy

ℹ️   Redundancy is described in detail in Section 6, "Redundancy".

5.10.1   Redundancy >> Firewall Redundancy

ℹ️   This menu is **not** available on the **FL MGUARD RS2000**.

5.10.1.1   Redundancy

Redundancy >> Firewall Redundancy >> Redundancy		
General	**Redundancy state**	Shows the current status.
	Enable redundancy	**No** (default): Firewall redundancy is disabled.
		Yes: Firewall redundancy is enabled.
		This function can only be activated when a suitable license key is installed.
		Further conditions apply if VPN redundancy is to be enabled at the same time, see "VPN redundancy" on page 311.
	Fail-over switching time	Maximum time that is allowed to elapse in the event of errors before switching to the other FL MGUARD.
	Waiting time prior to switching	**0 ... 10000 milliseconds, default: 0**
		Time the redundancy system ignores an error.
		The connectivity and availability checks ignore an error until it is still present after the time set here has elapsed.
	Priority of this device	**high/low**
		Specifies the priority associated with the presence notifications (CARP).
		Set the priority to **high** on the FL MGUARD that you want to be active. The FL MGUARD on standby is set to **low**.
		Both FL MGUARD devices in a redundant pair may either be set to different priorities or be assigned the **high** priority. .
		<table><tr><td>**i**</td><td>Never set **both** FL MGUARD devices in a redundant pair to **low** priority.</td></tr></table>

Redundancy >> Firewall Redundancy >> Redundancy		
	Passphrase for availability checks	On an FL MGUARD which is part of a redundant pair, checks are constantly performed to determine whether an active FL MGUARD is available and whether it should remain active. A variation of the CARP (Common Address Redundancy Protocol) is used here.
		CARP uses SHA-1 HMAC encryption together with a password. This password must be the same for both FL MGUARD devices. It is used for encryption and is never transmitted in plain text.

> **ℹ** The password is important for security since the FL MGUARD is vulnerable at this point. We recommend a password with at least 20 characters and numerous special characters (printable UTF-8 characters). It must be changed on a regular basis.

When changing the password, proceed as follows:

> **ℹ** Check the status of the set password before you enter a new one.

✓ There is only a valid password available and you are only permitted to enter a new password if you can see a **green check mark** to the right of the entry field.

Set the new password on both FL MGUARD devices. It does not matter which order you do this in but the same password must be used in both cases. If you inadvertently enter an incorrect password, follow the instructions under "How to proceed in the event of an incorrect password" on page 274.

As soon as a redundant pair has been assigned a new password, it automatically negotiates when it can switch to the new password without interruption.

The status is displayed using symbols. We recommend observing this status for security reasons.

A **red cross** indicates that the FL MGUARD has a new password that it wants to use. However, the old password is still in use.

A **yellow check mark** indicates that the new password is already in use but that the old password can still be accepted in case the other FL MGUARD still uses it.

If **no symbol** is shown, it means that no password is being used. For example, this may be because redundancy has not been activated or the firmware is booting up.

Redundancy >> Firewall Redundancy >> Redundancy

	If an FL MGUARD fails while the password is being changed, the following scenarios apply:
	– Password replacement has been started on all FL MGUARD devices and then interrupted because of a network error, for example. This scenario is rectified automatically.
	– Password replacement has been started on all FL MGUARD devices. However, an FL MGUARD then fails and must be replaced.
	Examine the remaining FL MGUARD to determine whether the process of changing the password has been completed. If you can see a green check mark, you must set the new password directly on the FL MGUARD that is being replaced.
	If you cannot see a green check mark, it means that the password has not yet been changed on the remaining FL MGUARD. In this case, you must change the password again on the FL MGUARD that is still in operation. Wait until the green check mark appears. Only then should you replace the FL MGUARD that has failed. Configure the replacement FL MGUARD with the new password immediately on setting up redundancy.
	– Password replacement has been started but not performed on all FL MGUARD devices because they have failed. Password replacement must be started as soon as a faulty FL MGUARD is back online. If an FL MGUARD has been replaced, it must first be configured with the old password before it is connected.

Redundancy >> Firewall Redundancy >> Redundancy		
	How to proceed in the event of an incorrect password	
	ⓘ	If you have inadvertently entered an incorrect password on an FL MGUARD, you cannot simply reenter the password using the correct one. Otherwise, in the event of adverse circumstances, this may result in both FL MGUARD devices being active.
	If you can still remember the old password, proceed as follows:	
	• Reconfigure the FL MGUARD on which the incorrect password was entered so that it uses the old password.	
	• Wait until the FL MGUARD indicates that the old password is being used.	
	• Then enter the correct password.	
	If you have forgotten the old password, proceed as follows:	
	• Check whether you can read the old password out from the other FL MGUARD.	
	• If the other FL MGUARD is disabled or missing, you can simply enter the correct new password on the active FL MGUARD on which you inadvertently set the incorrect password. Make sure that the other FL MGUARD is assigned the same password before operating it again.	
	• If the other FL MGUARD is already using the new password, you must make sure that the FL MGUARD with the incorrect password is not active or able to be activated, e.g., by removing the cable at the LAN or WAN interface.	
	In the case of remote access, you can enter a destination for the connectivity check that will not respond. Prior to provoking this kind of error, check that there is no redundancy error on any of the FL MGUARD devices. One FL MGUARD must be active and the other must be on standby. It might be necessary to rectify any errors displayed and only then use this method. After that, follow these steps:	
	– Replace the incorrect password with a different one.	
	– Enter this password on the active FL MGUARD too.	
	– Restart the FL MGUARD that is not active. You can do this, for example, by reconnecting the Ethernet cable or restoring the old settings for the connectivity check.	
Virtual interfaces	**External virtual Router ID**	**1, 2, 3, ... 255 (default: 51)**
		Only in Router network mode.
		This ID is sent by the redundant pair with each presence notification (CARP) via the external interface and is used to identify the redundant pair.
		This ID must be the same for both FL MGUARD devices. It is used to differentiate the redundant pair from other redundant pairs that are connected to the same Ethernet segment through their external interface.
		Please note that CARP uses the same protocol and port as VRRR (Virtual Router Redundancy Protocol). The ID set here must be different to the IDs on other devices which use VRRR or CARP and are located in the same Ethernet segment.

Redundancy >> Firewall Redundancy >> Redundancy		
	External virtual IP addresses	Default: 10.0.0.100
		Only in Router network mode.
		These are IP addresses which are shared by both FL MGUARD devices as virtual IP addresses of the external interface. These IP addresses must be the same for both FL MGUARD devices.
		These addresses are used as a gateway for explicit static routes for devices located in the same Ethernet segment as the external network interface of the FL MGUARD.
		The active FL MGUARD can receive ICMP queries via this IP address. It reacts to these ICMP requests depending on the menu settings under *Network Security* >> *Packet Filter* >> *Advanced* .
		No subnet masks or VLAN IDs are set up for the virtual IP addresses as these attributes are defined by the actual external IP address. For each virtual IP address, an actual IP address must be configured whose IP network accommodates the virtual address. The FL MGUARD transmits the subnet mask and VLAN setting from the actual external IP address to the corresponding virtual IP address.
		The applied VLAN settings define whether standard MTU settings or VLAN MTU settings are used for the virtual IP address.
		ⓘ Firewall redundancy cannot function correctly if no actual IP address and subnet mask are available.
	Internal virtual Router ID	**1, 2, 3, ... 255 (default: 51)**
		Only in Router network mode.
		This ID is sent by the redundant pair with each presence notification (CARP) via the external and internal interface and is used to identify the redundant pair.
		This ID must be set so it is the same for both FL MGUARD devices. It is used to differentiate the redundant pair from other Ethernet devices that are connected to the same Ethernet segment through their external/internal interface.
		Please note that CARP uses the same protocol and port as VRRR (Virtual Router Redundancy Protocol). The ID set here must be different to the IDs on other devices which use VRRR or CARP and are located in the same Ethernet segment.

Redundancy >> Firewall Redundancy >> Redundancy		
	Internal virtual IP addresses	As described under *External virtual IP addresses* , but with two exceptions.
		Under **Internal virtual IP addresses**, IP addresses are defined for devices which belong to the internal Ethernet segment. These devices must use the IP address as their default gateway. These addresses can be used as a DNS or NTP server when the FL MGUARD is configured as a server for the protocols.
		For each virtual IP address, an actual IP address must be configured whose IP network accommodates the virtual address.
		The response to ICMP requests with internal virtual IP addresses is independent from the settings made under *Network Security >> Packet Filter >> Advanced* .
Encrypted state synchronization	**Encrypt the state messages**	**Yes/No**
		If **Yes** is selected, the presence notifications for state synchronization are encrypted.
	Passphrase	The password is changed as described under "Passphrase for availability checks" on page 272.
		Only deviate from the prescribed approach if an incorrect password has been inadvertently entered.

How to proceed in the event of an incorrect password

i	If you have inadvertently entered an incorrect password on an FL MGUARD, you cannot simply reenter the password using the correct one. Otherwise, in the event of adverse circumstances, this may result in both FL MGUARD devices being active.

Case 1: Only one FL MGUARD has an incorrect password. The process of changing the password has not yet begun on the other FL MGUARD.

- Reconfigure the FL MGUARD on which the incorrect password was entered so that it uses the old password.
- Wait until the FL MGUARD indicates that the old password is being used.
- Then enter the correct password.

Case 2: The other FL MGUARD is already using the new password.

- The status of both FL MGUARD devices must be such that they are using an old password but expecting a new one (red cross). To ensure that this is the case, enter random passwords successively.
- Finally, generate a secure password and enter it on both FL MGUARD devices. This password is used immediately without any coordination.

During this process, the state of the FL MGUARD on standby may briefly switch to "outdated". However, this situation resolves itself automatically.

Redundancy >> Firewall Redundancy >> Redundancy		
	Encryption Algorithm	**DES, 3DES, AES-128, AES-192, AES-256**
		See "Algorithms" on page 247
	Hash Algorithm	**MD5, SH1, SHA-256, SHA-512**
		See "Algorithms" on page 247

5.10.1.2 Connectivity Checks

Targets can be configured for the internal and external interface in the connectivity check. It is important that these targets are actually connected to the specified interface. An ICMP echo reply cannot be received by an external interface when the corresponding target is connected to the internal interface (and vice versa). When the static routes are changed, the targets may easily not be checked properly.

Redundancy >> Firewall Redundancy >> Connectivity Checks		
External interface	**Kind of check**	Specifies whether a connectivity check is performed on the external interface, and if so, how.
		If **at least one target must respond** is selected, it does not matter whether the ICMP echo request is answered by the primary or secondary target.
		The request is only sent to the secondary target if the primary target did not offer a suitable answer. In this way, configurations can be supported where the devices are only optionally equipped with ICMP echo requests.
		If **all targets of one set must respond** is selected, then both targets must answer. If no secondary target is specified, then only the primary target must answer.
		If **Ethernet link detection only** is selected, then only the state of the Ethernet connection is checked.

Redundancy >> Firewall Redundancy >> Connectivity Checks		
	Primary targets for ICMP echo requests	This is an unsorted list of IP addresses used as targets for ICMP echo requests. We recommend using the IP addresses of routers, especially the IP addresses of default gateways or the actual IP address of the other FL MGUARD.
		Default: 10.0.0.30, 10.0.0.31 (for new addresses)
		Each set of targets for state synchronization can contain a maximum of ten targets.
	Secondary targets for ICMP echo requests	See above
		Only used if the check of the primary targets has failed.
		Failure of a secondary target is not detected in normal operation.
		Default: 10.0.0.30 (10.0.0.31 for new addresses)
		Each set of targets for state synchronization can contain a maximum of ten targets.
Internal interface	**Kind of check**	Specifies whether a connectivity check is performed on the internal interface, and if so, how.
		The settings are the same as those for the external interface.
	Primary targets for ICMP echo requests	See above
		Factory default: 192.168.1.30 (192.168.1.31 for new addresses)
	Secondary targets for ICMP echo requests	See above
		Factory default: 192.168.1.30 (192.168.1.31 for new addresses)

5.10.2 Redundancy >> FW Redundancy Status

5.10.2.1 Redundancy Status

Redundancy » FW Redundancy Status

Redundancy Status | **Connectivity Status**

Current State

State	B	T	O	A	C	R	Entry Time
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Wed Nov 9 11:59:13 CET 2011

Status of the Components

Component Type	Subject	State	Entry Time
Availability Check	External Interface	Received no CARP announcements from another mGuard.	Wed Oct 26 15:49:20 CEST 2011
Availability Check	Internal Interface	Received no CARP announcements from another mGuard.	Wed Oct 26 15:49:19 CEST 2011
Availability Check	Interface for State Synchronization	Received no CARP announcements from another mGuard.	Wed Oct 26 15:49:20 CEST 2011
Connectivity Check	External Interface	The check is **successful.**	Wed Nov 9 11:59:06 CET 2011
Connectivity Check	Internal Interface	The check is **successful.**	Wed Oct 26 15:49:17 CEST 2011
Phrase Swap Controller	Availability Check's Phrase	The configured phrase is in use.	Wed Oct 26 15:49:20 CEST 2011
Phrase Swap Controller	Phrase of the Encrypted State Synchronization	The configured phrase is in use.	Wed Oct 26 15:49:19 CEST 2011
State Replication	Connection Tracking Table	The database is **up to date.**	Wed Nov 9 11:59:13 CET 2011
State Replication	IPsec VPN Connections	The database is **up to date.**	Wed Nov 9 11:59:13 CET 2011
Virtual Interface Controller	Virtual Interface(s)	Forwarding of traffic is **allowed.**	Wed Nov 9 11:59:06 CET 2011

State History

State	B	T	O	A	C	R	Entry Time
active_waiting: The mGuard is actively forwarding and filtering network traffic. Additionally the mGuard waits for a restarting component.	+	+	-	t	s	?	Wed Nov 9 11:59:13 CET 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	+	t	s	u	Wed Nov 9 11:59:06 CET 2011
becomes_active: The mGuard becomes active.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
on_standby: The mGuard is on standby.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
outdated: The mGuard has an empty or outdated firewall or VPN state information which it wants to re-synchronize.	+	+	-	t	s	u	Wed Nov 9 11:59:06 CET 2011
faulty: The mGuard does not (yet) have proper connectivity or cannot determine it for sure.	+	+	-	t	f	u	Wed Nov 9 11:59:06 CET 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Thu Oct 27 11:33:40 CEST 2011
active_waiting: The mGuard is actively forwarding and filtering network traffic. Additionally the mGuard waits for a restarting component.	+	+	-	t	s	?	Thu Oct 27 11:33:39 CEST 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Thu Oct 27 11:33:33 CEST 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	+	t	s	u	Thu Oct 27 11:33:33 CEST 2011
becomes_active: The mGuard becomes active.	+	+	-	t	s	u	Thu Oct 27 11:33:32 CEST 2011
on_standby: The mGuard is on standby.	+	+	-	t	s	u	Thu Oct 27 11:33:32 CEST 2011
outdated: The mGuard has an empty or outdated firewall or VPN state information which it wants to re-synchronize.	+	+	-	t	s	u	Thu Oct 27 11:33:32 CEST 2011
faulty: The mGuard does not (yet) have proper connectivity or cannot determine it for sure.	+	+	-	t	f	u	Thu Oct 27 11:33:32 CEST 2011
active: The mGuard is actively forwarding and filtering network traffic.	+	+	-	t	s	u	Thu Oct 27 11:31:53 CEST 2011

Please note: The table is sorted chronologically starting with the youngest former state.

[Update]

Legend for column headers:
B: Flag indicating the booting state of the firmware.
T: Flag indicating the validity of the system time.

Redundancy >> FW Redundancy Status >> Redundancy Status		
Current State		Possible states:
		booting: The FL MGUARD is starting.
		faulty: The FL MGUARD is not (yet) connected properly.
		outdated: State synchronization of the databases is not (yet) up-to-date.
		on_standby: The FL MGUARD is ready for activation if the other FL MGUARD fails.
		becomes_active: The FL MGUARD is becoming active because the other FL MGUARD has failed.
		active: The FL MGUARD is active.
		becomes_standby: The FL MGUARD is switching from the active state to standby mode. The state is changed to *outdated* since the status database has to be updated first.
Status of the Components	**Availability Check**	Relates to the status of the availability check for the internal or external interface.
		The availability check has three possible results.
		– Presence notifications (CARP) are not received from any other FL MGUARD device.
		– Another FL MGUARD is available which is to become or remain active.
		– Another FL MGUARD is available which is active but is to go "on_standby".
	Connectivity Check	Indicates whether the check was successful.
		Each interface is checked separately.
	State Replication	When synchronizing the state, various databases are checked to see whether everything is up-to-date. With one redundant pair, only one database is active while the other is on standby. Any change made to this state is also displayed.
		– The **Connection Tracking Table** relates to the firewall state database.
		– **IPsec VPN Connections** (with activated VPN redundancy)
	Virtual Interface Controller	All virtual interfaces are checked together to see whether the forwarding of packets is allowed.

Redundancy >> FW Redundancy Status >> Redundancy Status				
State History				The table starts with the most recent state.
				The abbreviations are as follows:
	B	**Firmware status**	**+**	Firmware started up completely
			-	Firmware not yet started up completely
	T	**System time**	**+**	Valid system time
			-	Invalid system time
	O	**Timeout of the previous state**	**+**	Timeout
			-	No timeout
	A	**Availability check**	**?**	Unknown state
			s	Another FL MGUARD is available. This FL MGUARD is active (or is currently being enabled).
			f	Another FL MGUARD is available. This FL MGUARD is on standby (or is currently switching to standby).
			t	No other FL MGUARD available
	C	**Connectivity check**	**?**	Unknown state
			s	Check of all components was successful
			f	Check of at least one component has failed
	R	**State synchronization**	**?**	Unknown state
			u	Database is up-to-date
			o	Database is obsolete
			-	Database switching to "on_standby"
			+	Database switching to "active"

5.10.2.2   Connectivity Status

Redundancy >> FW Redundancy Status >> Connectivity Status			
External Interface	**Summarized result**	**success/fail**	
		Result of the connectivity check for the external interface.	
		The **fail** result is also displayed until the specific result of the connectivity check is known.	
		The last two intervals of the connectivity check are taken into consideration for the combined result. **success** is only displayed if both were successful.	
		success (longer due to waiting time) is displayed, if the time an error was present was shorter than set under *"Waiting time prior to switching"* in the *Redundancy >> Firewall Redundancy >> Redundancy* menu.	
	Ethernet link status	Shows whether the Ethernet connection has been established.	
	Number of check intervals	Number of completed check intervals. When the counter is full, a message is displayed in front of the number.	
	Kind of check	Repeats the setting for the connectivity check (see *Kind of check* on Page 278).	

Redundancy >> FW Redundancy Status >> Connectivity Status		
	Check interval	Shows the time (in milliseconds) between the starts of the checks.
		This value is calculated from the set fail-over switching time.
	Timeout per interval and set of targets	Shows the time (in milliseconds) after which a target is classed as "no response" if no response to the ICMP echo request has been received.
		This value is calculated from the set fail-over switching time.
	Waiting time prior to reporting an error (except for link errors)	Time the redundancy system ignores an error.
		The connectivity and availability checks ignore an error until it is still present after the time set here has elapsed.
		This value is set under *"Waiting time prior to switching"* in the *Redundancy >> Firewall Redundancy >> Redundancy* menu.
	Results of the last 16 intervals (youngest first)	A green plus indicates a successful check.
		A red minus indicates a failed check.
	Results of the primary targets	Only visible when a primary target is set (see *Primary targets for ICMP echo requests* on Page 278).
		Shows the results of the ICMP echo requests in chronological order. The most recent result is at the front.
		"sR" indicates a cycle during which ICMP echo requests have been correctly transmitted and received. Missing answers are indicated by a "/" and requests that have not been transmitted are indicated by a "_".
	Results of the secondary targets	Only visible when a secondary target is set (see *Secondary targets for ICMP echo requests* on Page 278).
Internal Interface	**Summarized result**	See *External Interface*
	Ethernet link status	See *External Interface*
	Number of check intervals	See *External Interface*
	Check interval	See *External Interface*
	Timeout per interval and set of targets	See *External Interface*
	Results of the last 16 intervals (youngest first)	See *External Interface*

5.10.3 Ring/Network Coupling

5.10.3.1 Ring/Network Coupling
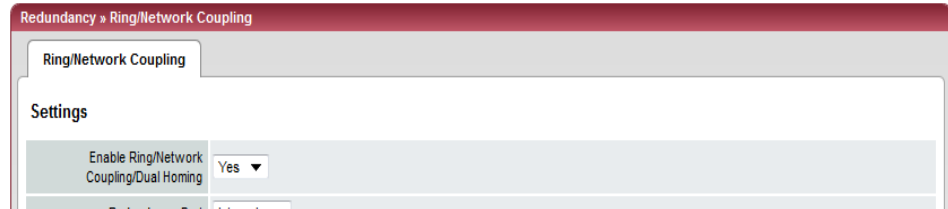
Redundancy >> Firewall Redundancy >> Ring/Network Coupling		
Settings	**Enable Ring/Network Coupling/Dual Homing**	**Yes/No** When activated, the status of the Ethernet connection is transmitted from one port to another in Stealth mode. This means that interruptions in the network can be traced easily.
	Redundancy Port	**Internal/External** **Internal**: If the connection is lost/established on the LAN port, the WAN port is also disabled/enabled. **External**: If the connection is lost/established on the WAN port, the LAN port is also disabled/enabled.

5.11 Logging menu

Logging refers to the recording of event messages, e.g., regarding settings that have been made, the application of firewall rules, errors, etc.

Log entries are recorded in various categories and can be sorted and displayed according to these categories (see "Logging >> Browse local logs" on page 287).

5.11.1 Logging >> Settings

5.11.1.1 Remote Logging

All log entries are recorded in the main memory of the FL MGUARD by default. Once the maximum memory space for log entries has been used up, the oldest log entries are automatically overwritten by new entries. In addition, all log entries are deleted when the FL MGUARD is switched off.

To prevent this, log entries (SysLog messages) can be transmitted to an external computer (SysLog server). This is particularly useful if you wish to manage the logs of multiple FL MGUARD devices centrally.

Logging >> Remote Logging			
Settings	**Activate remote UDP logging**	**Yes/No**	
		If you want all log entries to be transmitted to the external log server (specified below), select **Yes**.	
	Log Server IP address	Specify the IP address of the log server to which the log entries should be transmitted via UDP.	
		An IP address must be specified, not a host name. This function does not support name resolution because it might not be possible to make log entries if a DNS server failed.	
	Log Server port (normally 514)	Specify the port of the log server to which the log entries should be transmitted via UDP. Default: 514	

> ℹ️ If SysLog messages should be transmitted to a SysLog server via a VPN channel, the IP address of the SysLog server must be located in the network that is specified as the **Remote** network in the definition of the VPN connection.
>
> The internal IP address (in Stealth mode: **Stealth Management IP Address** or **Virtual IP**) must be located in the network that is specified as **Local** in the definition of the VPN connection (see "Defining a VPN connection/VPN connection channels" on page 223).

Logging >> Remote Logging [...]

– If the Enable 1-to-1 NAT of the local network to an internal network option is set to Yes (see "1:1 NAT" on page 236), the following applies:

The internal IP address (in Stealth mode: **Stealth Management IP Address** or **Virtual IP**) must be located in the network that is specified as the **Internal network address for local 1-to-1 NAT**.

– If the Enable 1-to-1 NAT of the remote network to a different network option is set to Yes (see "1:1 NAT" on page 236), the following applies:

The IP address of the SysLog server must be located in the network that is specified as **Remote** in the definition of the VPN connection.

5.11.2 Logging >> Browse local logs

The corresponding checkboxes for filtering entries according to their category are displayed below the log entries, depending on which FL MGUARD functions were active.

To display one or more categories, enable the checkboxes for the desired categories and click on **Reload logs**.

5.11.2.1 Log entry categories

General

Log entries that cannot be assigned to other categories.

Network Security

$\boxed{\mathbf{i}}$ | In the case of the **FL MGUARD RS2000**, access via its firewall is **not** logged.

Logged events are shown here if the logging of firewall events was selected when defining the firewall rules (Log = Yes).

Log ID and number for tracing errors

Log entries that relate to the firewall rules listed below have a log ID and number. This log ID and number can be used to trace the firewall rule to which the corresponding log entry relates and that led to the corresponding event.

Firewall rules and their log ID

– Packet filters:
  Network Security >> Packet Filter >> Incoming Rules menu
  Network Security >> Packet Filter >> Outgoing Rules menu
  Log ID: *fw-incoming* or *fw-outgoing*
– Firewall rules for VPN connections:
  IPsec VPN >> Connections >> Edit >> Firewall menu, Incoming/Outgoing
  Log ID: *vpn-fw-in* or *vpn-fw-out*
– Firewall rules for web access to the FL MGUARD via HTTPS:
  Management >> Web Settings >> Access menu
  Log ID: *fw-https-access*
– Firewall rules for access to the FL MGUARD via SNMP:
  Management >> SNMP >> Query menu
  Log ID: *fw-snmp-access*
– Firewall rules for SSH remote access to the FL MGUARD:
  Management >> System Settings >> Shell Access menu
  Log ID: *fw-ssh-access*
– Firewall rules for the user firewall:
  Network Security >> User Firewall menu, Firewall rules
  Log ID: *ufw-*
– Rules for NAT, port forwarding:
  Network >> NAT >> IP and Port Forwarding menu

  Log ID: *fw-portforwarding*
– Firewall rules for the serial interface:
  Network >> Interfaces >> Dial-in menu
  Incoming rules
  Log ID: *fw-serial-incoming*
  Outgoing rules
  Log ID: *fw-serial-outgoing*

Searching for firewall rules on the basis of a network security log

If the **Network Security** checkbox is enabled so that the relevant log entries are displayed, the **Jump to firewall rule** search field is displayed below the *Reload logs* button.

Proceed as follows if you want to trace the firewall rule referenced by a log entry in the *Network Security* category and which resulted in the corresponding event:

1. Select the section that contains the log ID and number in the relevant log entry, for example: fw-https-access-1-1ec2c133-dca1-1231-bfa5-000cbe01010a
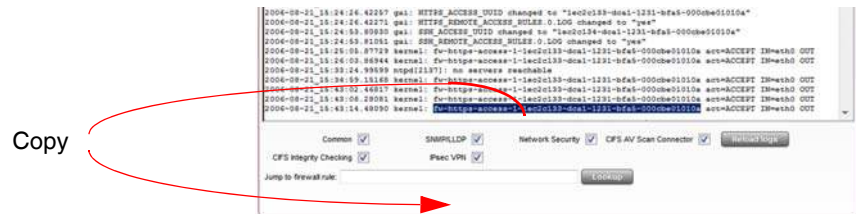
2. Copy this section into the **Jump to firewall rule** field.
3. Click on **Lookup**.
   The configuration page containing the firewall rule that the log entry refers to is displayed.

CIFS AV Scan Connector

This log contains CIFS server messages. This server is used by the FL MGUARD itself for enabling purposes.

In addition, messages that occur when connecting the network drives and are grouped together and provided by the CIFS server are also visible.

CIFS Integrity Checking

Messages relating to the integrity check of network drives are displayed in this log.

In addition, messages that occur when connecting the network drives and are required for the integrity check are also visible.

DHCP server/relay

Messages from the services defined under "Network -> DHCP".

SNMP/LLDP

Messages from services defined under "Management -> SNMP".

IPsec VPN

Lists all VPN events.

The format corresponds to standard Linux format.

There are special evaluation programs that present information from the logged data in a more easily readable format.

5.12 Support menu

5.12.1 Support >> Tools

5.12.1.1 Ping Check

Support >> Tools >> Ping Check	
Ping Check	**Aim**: To check whether a partner can be accessed via a network. **Procedure**: • Enter the IP address or host name of the partner in the **Hostname/IP Address** field. Then click on **Ping**. A corresponding message is then displayed.

5.12.1.2 Traceroute

Support >> Tools >> Traceroute	
Traceroute	**Aim**: To determine which intermediate points or routers are located on the connection path to a partner. **Procedure**: • Enter the host name or IP address of the partner whose route is to be determined in the **Hostname/IP Address** field. • If the points on the route are to be output with IP addresses instead of host names (if applicable), activate the **Do not resolve IP addresses to hostnames** checkbox. • Then click on **Trace**. A corresponding message is then displayed.

5.12.1.3 DNS Lookup
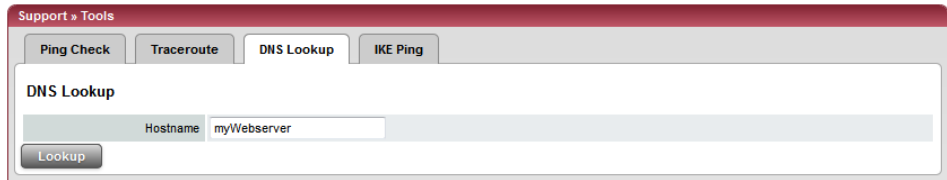
Support >> Tools >> DNS Lookup	
DNS Lookup	**Aim**: To determine which host name belongs to a specific IP address or which IP address belongs to a specific host name. **Procedure**: • Enter the IP address or host name in the **Hostname** field. • Click on **Lookup**. The response, which is determined by the FL MGUARD according to the DNS configuration, is then returned.

5.12.1.4 IKE Ping
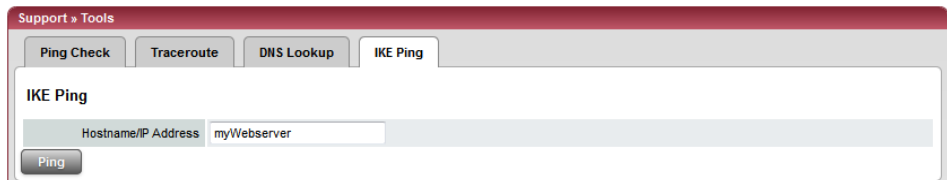
Support >> Tools >> IKE Ping	
IKE Ping	**Aim**: To determine whether the VPN software for a VPN gateway is able to establish a VPN connection, or whether a firewall prevents this, for example. **Procedure**: • Enter the name or IP address of the VPN gateway in the **Hostname/IP Address** field. • Click on **Ping**. • A corresponding message is then displayed.

5.12.2   Support >> Advanced

5.12.2.1   Hardware

This page lists various hardware properties of the FL MGUARD.

Support » Advanced	
Hardware Information	
Hardware	Innominate mGuard centerport
CPU	QEMU Virtual CPU version 0.12.5
CPU Family	x86_64
CPU Stepping	3
CPU Clock Speed	2393 MHz
System Uptime	50 days, 2:04
User Space Memory	123856 kB
MAC 1	00:0c:be:06:00:f0
MAC 2	00:0c:be:06:00:f1
MAC 3	00:0c:be:06:00:f2
MAC 4	00:0c:be:06:00:f3
Product Name	Innominate mGuard VirtualBox
OEM Name	Innominate
OEM Serial Number	1A715030
Serial Number	1A715030
Flash ID	U3DDD33F8-0B67-1A85-8E4B-027ABDA00853
Hardware Version	00002001
Version Parameterset	4
Version of the bootloader	bootloader_0-1.3.0.default
Version of the rescue system	rescue_0-1.7.0.default
Current root filesystem	rootfs1

5.12.2.2   Snapshot

This function is used for support purposes.

Support » Advanced	
Support Snapshot	
Download	This will create a snapshot of the mGuard for support purposes.
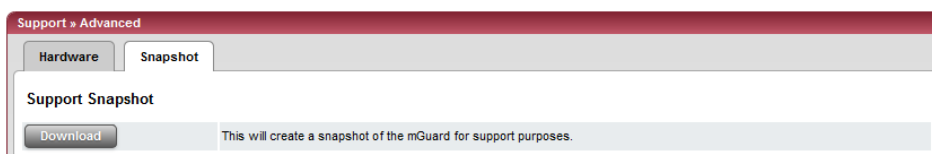
It creates a compressed file (in tar.gz format) containing all active configuration settings and log entries that could be relevant for error diagnostics.

> ℹ This file does not contain any private information such as private machine certificates or passwords. However, any pre-shared keys of VPN connections are contained in the snapshots.

To create a snapshot, proceed as follows:

- Click on **Download**.
- Save the file (under the name "snapshot.tar.gz").

Provide the file to the support team of your dealer, if required.

5.13   CIDR (Classless Inter-Domain Routing)

IP subnet masks and CIDR are methods of notation that combine several IP addresses to create a single address area. An area comprising consecutive addresses is handled like a network.

To specify an area of IP addresses for the FL MGUARD, e.g., when configuring the firewall, it may be necessary to specify the address area in CIDR format. In the table below, the left-hand column shows the IP subnet mask, while the right-hand column shows the corresponding CIDR notation.

IP subnet mask	Binary				CIDR
255.255.255.255	11111111	11111111	11111111	11111111	32
255.255.255.254	11111111	11111111	11111111	11111110	31
255.255.255.252	11111111	11111111	11111111	11111100	30
255.255.255.248	11111111	11111111	11111111	11111000	29
255.255.255.240	11111111	11111111	11111111	11110000	28
255.255.255.224	11111111	11111111	11111111	11100000	27
255.255.255.192	11111111	11111111	11111111	11000000	26
255.255.255.128	11111111	11111111	11111111	10000000	25
255.255.255.0	11111111	11111111	11111111	00000000	24
255.255.254.0	11111111	11111111	11111110	00000000	23
255.255.252.0	11111111	11111111	11111100	00000000	22
255.255.248.0	11111111	11111111	11111000	00000000	21
255.255.240.0	11111111	11111111	11110000	00000000	20
255.255.224.0	11111111	11111111	11100000	00000000	19
255.255.192.0	11111111	11111111	11000000	00000000	18
255.255.128.0	11111111	11111111	10000000	00000000	17
255.255.0.0	11111111	11111111	00000000	00000000	16
255.254.0.0	11111111	11111110	00000000	00000000	15
255.252.0.0	11111111	11111100	00000000	00000000	14
255.248.0.0	11111111	11111000	00000000	00000000	13
255.240.0.0	11111111	11110000	00000000	00000000	12
255.224.0.0	11111111	11100000	00000000	00000000	11
255.192.0.0	11111111	11000000	00000000	00000000	10
255.128.0.0	11111111	10000000	00000000	00000000	9
255.0.0.0	11111111	00000000	00000000	00000000	8
254.0.0.0	11111110	00000000	00000000	00000000	7
252.0.0.0	11111100	00000000	00000000	00000000	6
248.0.0.0	11111000	00000000	00000000	00000000	5
240.0.0.0	11110000	00000000	00000000	00000000	4
224.0.0.0	11100000	00000000	00000000	00000000	3
192.0.0.0	11000000	00000000	00000000	00000000	2
128.0.0.0	10000000	00000000	00000000	00000000	1

Example: 192.168.1.0/255.255.255.0 corresponds to CIDR: 192.168.1.0/24

5.14   Network example diagram

The following diagram shows how IP addresses can be distributed in a local network with subnetworks, which network addresses result from this, and how the details regarding additional internal routes may look for the FL MGUARD.

Internet

External address, e.g., 123.456.789.21
(assigned by the Internet service provider)

FL MGUARD in *Router* network mode
Internal address of the FL MGUARDs: 192.168.11.1

Switch

Network A

Network address: 192.168.11.0/24

Subnet mask: 255.255.255.0

A1 A2 A3 A4 A5

Router

External IP address:
192.168.11.2

Internal IP address:
192.168.15.254

Subnet mask:
255.255.255.0

Router

Switch

Network B

Network address:
192.168.15.0/24

Subnet mask: 255.255.255.0

B1 B2 B3 B4

Router

External IP address:
192.168.15.1

Internal IP address:
192.168.27.254

Subnet mask:
255.255.255.0

Router

Switch

Network C

Network address:
192.168.27.0/24

Subnet mask: 255.255.255.0

= Additional internal routes

C1 C2 C3 C4

Network A	Computer	A1	A2	A3	A4	A5
	IP address	192.168.11.3	**192.168.11.4**	**192.168.11.5**	**192.168.11.6**	**192.168.11.7**
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**
Network B	Computer	B1	B2	B3	B4	Additional internal routes
	IP address	192.168.15.2	**192.168.15.3**	**192.168.15.4**	**192.168.15.5**	Network: 192.168.15.0/24 Gateway: 192.168.11.2
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	Network: 192.168.27.0/24 Gateway: 192.168.11.2
Network C	Computer	C1	C2	C3	C4	
	IP address	192.168.27.1	**192.168.27.2**	**192.168.27.3**	**192.168.27.4**	
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	

6 Redundancy

![info icon] The firewall and VPN redundancy functions are **not** available on the **FL MGUARD RS2000**.

There are several different ways of compensating for errors using the FL MGUARD so that an existing connection is not interrupted.

–   **Firewall redundancy:** Two identical FL MGUARD devices can be combined to form a redundant pair, meaning one takes over the functions of the other if an error occurs.
–   **VPN redundancy**: An existing firewall redundancy forms the basis for VPN redundancy. In addition, the VPN connections are designed so that at least one FL MGUARD in a redundant pair operates the VPN connections.
–   **Ring/network coupling**: In ring/network coupling, another method is used. Parts of a network are designed as redundant. In the event of errors, the alternative path is selected.

6.1 Firewall redundancy

Using firewall redundancy, it is possible to combine two identical FL MGUARD devices into a redundant pair (single virtual router). One FL MGUARD takes over the functions of the other if an error occurs. Both FL MGUARD devices run synchronously, meaning an existing connection is not interrupted when the FL MGUARD is switched.
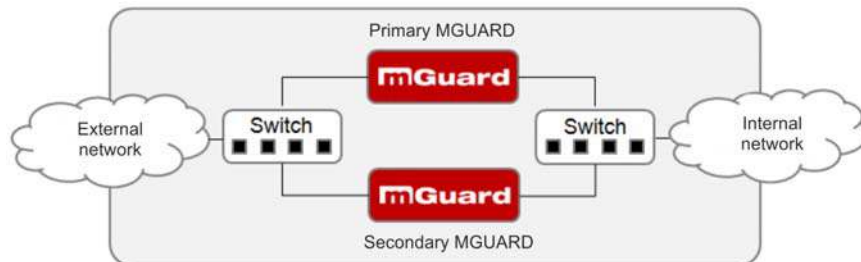
Figure 6-1   Firewall redundancy (example)

Basic requirements for firewall redundancy

![info icon] A license is required for the firewall redundancy function. It can only be used if the corresponding license has been purchased and installed.

–   Only identical FL MGUARD devices can be used together in a redundant pair.
–   In Router network mode, firewall redundancy is only supported with the "static" Router mode.
–   The Stealth network mode is currently not supported.
–   For further restrictions, see "Requirements for firewall redundancy" on page 300 and "Limits of firewall redundancy" on page 310.

6.1.1 Components in firewall redundancy

Firewall redundancy is comprised of several components:

– **Connectivity check**

Checks whether the necessary network connections have been established.

– **Availability check**

Checks whether an active FL MGUARD is available and whether this should remain active.

– **State synchronization of the firewall**

The FL MGUARD on standby receives a copy of the current firewall database state.

– **Virtual network interface**

Provides virtual IP addresses and MAC addresses that can be used by other devices as routes and default gateways.

– **State monitoring**

Coordinates all components.

– **Status indicator**

Shows the user the state of the FL MGUARD.

Connectivity check

On each FL MGUARD in a redundant pair, checks are constantly made as to whether a connection is established through which the network packets can be forwarded.

Each FL MGUARD checks its own internal and external network interfaces independently of each other. Both interfaces are tested for a continuous connection. This connection must be in place, otherwise the connectivity check will fail.

ICMP echo requests can also be sent (optional). The ICMP echo requests can be set using the *Redundancy >> Firewall Redundancy >> Connectivity Checks* menu.

Availability check

On each FL MGUARD in a redundant pair, checks are also constantly performed to determine whether an active FL MGUARD is available and whether it should remain active. A variation of the CARP (Common Address Redundancy Protocol) is used here.

The active FL MGUARD constantly sends presence notifications through its internal and external network interface while both FL MGUARD devices listen. If a dedicated Ethernet link for state synchronization of the firewall is available, the presence notification is also sent via this link. In this case, the presence notification for the external network interface can also be suppressed.

The availability check fails if an FL MGUARD does not receive any presence notifications within a certain time. The check also fails if an FL MGUARD receives presence notifications with a lower priority than its own.

The data is always transmitted through the physical network interface and never through the virtual network interface.

State synchronization

The FL MGUARD on standby receives a copy of the state of the FL MGUARD that is currently active.

This includes a database containing the forwarded network connections. This database is filled and updated constantly by the forwarded network packets. It is protected against unauthorized access. The data is transmitted through the physical LAN interface and never through the virtual network interface.

To keep internal data traffic to a minimum, a VLAN can be configured to store the synchronization data in a separate multicast and broadcast domain.

Virtual IP addresses

Each FL MGUARD is configured with virtual IP addresses. The number of virtual IP addresses depends on the network mode used. Both FL MGUARD devices in a redundant pair must be assigned the same virtual IP addresses. The virtual IP addresses are required by the FL MGUARD to establish virtual network interfaces.

Two virtual IP addresses are required in Router network mode, while others can be created. One virtual IP address is required for the external network interface and the other for the internal network interface.

These IP addresses are used as a gateway for routing devices located in the external or internal LAN. In this way, the devices can benefit from the high availability resulting from the use of both redundant FL MGUARD devices.

The redundant pair automatically defines MAC addresses for the virtual network interface. These MAC addresses are identical for the redundant pair. In Router network mode, both FL MGUARD devices share a MAC address for the virtual network interface connected to the external and internal Ethernet segment.

In Router network mode, the FL MGUARD devices support forwarding of special UDP/TCP ports from a virtual IP address to other IP addresses, provided the other IP addresses can be reached by the FL MGUARD. In addition, the FL MGUARD also masks data with virtual IP addresses when masquerading rules are set up.

State monitoring

State monitoring is used to determine whether the FL MGUARD is active, on standby or has an error. Each FL MGUARD determines its own state independently, depending on the information provided by other components. State monitoring ensures that two FL MGUARD devices are not active at the same time.

Status indicator

The status indicator contains detailed information on the firewall redundancy state. A summary of the state can be called up using the *Redundancy >> Firewall Redundancy >> Redundancy* or *Redundancy >> Firewall Redundancy >> Connectivity Checks* menus.

6.1.2 Interaction of the firewall redundancy components

During operation, the components work together as follows: Both FL MGUARD devices perform ongoing connectivity checks for both of their network interfaces (internal and external). In addition, an ongoing availability check is performed. Each FL MGUARD listens continuously for presence notifications (CARP) and the active FL MGUARD also sends them.

Based on the information from the connectivity and availability checks, the state monitoring function is made aware of the state of the FL MGUARD devices. State monitoring ensures that the active FL MGUARD mirrors its data onto the other FL MGUARD (state synchronization).

6.1.3 Firewall redundancy settings from previous versions

Existing configuration profiles on firmware version 6.1.x (and earlier) can be imported with certain restrictions. For information, please contact Innominate.

6.1.4 Requirements for firewall redundancy

– The firewall redundancy function can only be activated when a suitable license key is installed.
   (See under: *Redundancy >> Firewall Redundancy >> Redundancy >> Enable redundancy)*
– Each set of targets for the connectivity check can contain more than ten targets (a fail-over time cannot be guaranteed without an upper limit).
   Redundancy >> Firewall Redundancy >> Redundancy
   – *>> External Interface >> Primary targets for ICMP echo requests*
   – *>> External Interface >> Secondary targets for ICMP echo requests*
   – *>> Internal interface >> Primary targets for ICMP echo requests*
   – *>> Internal interface >> Secondary targets for ICMP echo requests*
   If "**at least one target must respond**" or "**all targets of one set must respond**" is selected under *External Interface >> Kind of check* , then *External Interface >> Primary targets for ICMP echo requests* cannot be left empty. This also applies to the internal interface.
– In **Router network mode**, at least one external and one internal virtual IP address must be set. A virtual IP address cannot be listed twice.

6.1.5 Fail-over switching time

The FL MGUARD calculates the intervals for the connectivity check and availability check automatically according to the variables under **Fail-over switching time**.

Connectivity check

The factors which define the intervals for the connectivity check are specified in Table 6-1 on Page 301.

64-kbyte ICMP echo requests are sent for the connectivity check. They are sent on layer 3 of the Internet protocol. When VLAN is not used, 18 bytes for the MAC header and checksum are added to this with the Ethernet on layer 2. The ICMP echo reply is the same size.

The bandwidth is also shown in Table 6-1. This takes into account the values specified for a single target and adds up the bytes for the ICMP echo request and reply.

The timeout on the FL MGUARD following transmission includes the following:
– The time required by the FL MGUARD to transmit an ICMP echo reply. If other data traffic is expected, the half-duplex mode is not suitable here.
– The time required for the transmission of the ICMP echo request to a target. Consider the latency during periods of high capacity utilization. This applies especially when routers forward the request.
– The time required on each target for processing the request and transmitting the reply to the Ethernet layer. Please note that the full-duplex mode is also used here.
– The time for transmission of the ICMP echo reply to the FL MGUARD.

Table 6-1　　　Frequency of the ICMP echo requests

Fail-over switching time	ICMP echo requests per target	Timeout on the FL MGUARD after transmission	Bandwidth per target
1 s	10 per second	100 ms	6560 bps
3 s	3.3 per second	300 ms	2187 bps
10 s	1 per second	1 s	656 bps

If secondary targets are configured, then additional ICMP echo requests may occasionally be sent to these targets. This must be taken into account when calculating the ICMP echo request rate.

The timeout for a single ICMP echo request is displayed in Table 6-1. This does not indicate how many of the responses can be missed before the connectivity check fails. The check tolerates a negative result for one of two back-to-back intervals.

Availability check

Presence notifications (CARP) measure up to 76 bytes on layer 3 of the Internet protocol. When VLAN is not used, 18 bytes for the MAC header and checksum are added to this with the Ethernet on layer 2. The ICMP echo reply is the same size.

Table 6-2 shows the maximum frequency at which the presence notifications (CARP) are sent from the active FL MGUARD. It also shows the bandwidth used in the process. The frequency depends on the FL MGUARD priority and the *Fail-over switching time* .

Table 6-2 also shows the maximum latency tolerated by the FL MGUARD for the network that is used to transmit the presence notifications (CARP). If this latency is exceeded, the redundant pair can exhibit undefined behavior.

Table 6-2   Frequency of the presence notifications (CARP)

Fail-over switching time	Presence notifications (CARP) per second		Maximum latency	Bandwidth on layer 2 for the high priority
	High priority	**Low priority**		
1 s	50 per second	25 per second	20 ms	37.60 bps
3 s	16.6 per second	8.3 per second	60 ms	12.533 bps
10 s	5 per second	2.5 per second	200 ms	3.76 bps

6.1.6   Error compensation through firewall redundancy

Firewall redundancy is used to compensate for hardware failures.
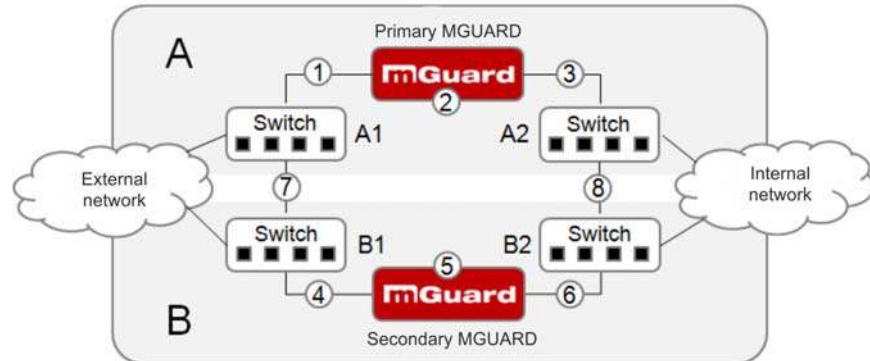
Figure 6-2   Possible error locations (1 ... 8)

Figure 6-2 shows a diagram containing various error locations (not related to the network mode)

Each of the FL MGUARD devices in a redundant pair is located in a different area (A and B). The FL MGUARD in area A is connected to switch A1 through its external Ethernet interface and to switch A2 through its internal Ethernet interface. FL MGUARD B is connected accordingly to switches B1 and B2. In this way, the switches and FL MGUARD devices connect an external Ethernet network to an internal Ethernet network. The connection is established by forwarding network packets (in Router network mode).

Firewall redundancy compensates for errors displayed in Figure 6-2 if only one occurs at any given time. If two errors occur simultaneously, they are only compensated if they occur in the same area (A or B).

For example, if one of the FL MGUARD devices fails completely due to a power outage, then this is detected. A connection failure is compensated if the connection fails completely or partially. When the connectivity check is set correctly, a faulty connection caused by the loss of data packets or an excessive latency is detected and compensated . Without the connectivity check, the FL MGUARD cannot determine which area caused the error.

A connection failure between switches on a network side (internal/external) is not compensated for (7 and 8 in Figure 6-2).

6.1.7 Handling firewall redundancy in extreme situations

i | The situations described here only occur rarely.

Restoration in the event of a network lobotomy

A network lobotomy occurs if a redundant pair is separated into two FL MGUARD devices operating independently of one another. In this case, each FL MGUARD deals with its own tracking information as the two FL MGUARD devices can no longer communicate via layer 2. A network lobotomy can be triggered by a rare and unfortunate combination of network settings, network failures, and firewall redundancy settings.

Each FL MGUARD is active during a network lobotomy. The following occurs after the network lobotomy has been rectified: If the FL MGUARD devices have different priorities, the FL MGUARD with the higher priority becomes active and the other switches to standby. If both FL MGUARD devices have the same priority, an identifier sent with the presence notifications (CARP) determines which FL MGUARD becomes active.

Both FL MGUARD devices manage their own firewall state during the network lobotomy. The active FL MGUARD retains its state. Connections on the other FL MGUARD, which were established during the lobotomy, are dropped.

Fail-over when establishing complex connections

Complex connections are network protocols which are based on different IP connections. One example of this is the FTP protocol. In an FTP protocol, the client establishes a control channel for a TCP connection. The server is then expected to open another TCP connection over which the client can then transmit data. The data channel on port 20 of the server is set up while the control channel on port 21 of the server is being established.

If the relevant connection tracking function is activated on the FL MGUARD (see "Advanced" on page 188), complex connections of this type are tracked. In this case, the administrator only needs to create a firewall rule on the FL MGUARD which allows the client to establish a control channel to the FTP server. The FL MGUARD enables the server to establish a data channel automatically, regardless of whether the firewall rules allow for this.

The tracking of complex connections is part of the firewall state synchronization process. However, to keep the latency short, the FL MGUARD forwards the network packets independently from the firewall state synchronization update that has been triggered by the network packets themselves.

Therefore, it may be the case for a very brief period that a state change for the complex connection is not forwarded to the FL MGUARD on standby if the active FL MGUARD fails. In this case, tracking of the connection to the FL MGUARD which is active after the fail-over is not continued correctly. This cannot be corrected by the FL MGUARD. The data link is then reset or interrupted.

Fail-over when establishing semi-unidirectional connections

A semi-unidirectional connection refers to a single IP connection (such as UDP connections) where the data only travels in one direction after the connection is established with a bidirectional handshake.

The data flows from the responder to the initiator. The initiator only sends data packets at the very start.

The following applies only to certain protocols which are based on UDP. Data always flows in both directions on TCP connections.

If the firewall of the FL MGUARD is set up to only accept data packets from the initiator, the firewall accepts all related responses per se. This happens regardless of whether or not a relevant firewall rule is available.

A scenario is conceivable in which the FL MGUARD allows the initiating data packet to pass through and then fails before the relevant connection entry has been made in the other FL MGUARD. The other FL MGUARD may then reject the responses as soon as it becomes the active FL MGUARD.

The FL MGUARD cannot correct this situation due to the single-sided connection. As a countermeasure, the firewall can be configured so that the connection can be established in both directions. This is normally already handled via the protocol layer and no additional assignment is required.

Loss of data packets during state synchronization

If data packets are lost during state synchronization, this is detected automatically by the FL MGUARD, which then requests the active FL MGUARD to send the data again.

This request must be answered within a certain time, otherwise the FL MGUARD on standby is assigned the "outdated" state and asks the active FL MGUARD for a complete copy of all state information.

The response time is calculated automatically from the fail-over switching time. This is longer than the time for presence notifications (CARP), but shorter than the upper limit of the fail-over switching time.

Loss of presence notifications (CARP) during transmission

A one-off loss of presence notifications (CARP) is tolerated by the FL MGUARD, but it does not tolerate the loss of subsequent presence notifications (CARP). This applies to the availability check on each individual network interface, even when these are checked simultaneously. It is therefore very unlikely that the availability check will fail as a result of a very brief network interruption.

Loss of ICMP echo requests/replies during transmission

ICMP echo requests or replies are important for the connectivity check. Losses are always observed, but are tolerated under certain circumstances.

The following measures can be used to increase the tolerance level on ICMP echo requests.
– Select **at least one target must respond** under **Kind of check** in the *Redundancy >> Firewall Redundancy >> Connectivity Checks* menu.
– Also define a secondary set of targets here. The tolerance level for the loss of ICMP echo requests can be further increased by entering the targets of unreliable connections under both sets (primary and secondary) or listing them several times within a set.

Restoring the primary FL MGUARD following a failure

If a redundant pair is defined with different priorities, the secondary FL MGUARD becomes active if the connection fails. The primary FL MGUARD becomes active again after the failure has been rectified. The secondary FL MGUARD receives a presence notification (CARP) and returns to standby mode.

State synchronization

If the primary FL MGUARD becomes active again after a failure of the internal network connection, the FL MGUARD may contain an obsolete copy of the firewall database.. This database must, therefore, be updated before the connection is reestablished. The primary FL MGUARD ensures that it receives an up-to-date copy before becoming active.

6.1.8   Interaction with other devices

Virtual and actual IP addresses

With firewall redundancy in Router network mode, the FL MGUARD uses actual IP addresses to communicate with other network devices.

Virtual IP addresses are used in the following two cases:
–   Virtual IP addresses are used when establishing and operating VPN connections.
–   If DNS and NTP services are used according to the configuration, they are offered to internal virtual IP addresses.

The usage of actual (management) IP addresses is especially important for the connectivity check and availability check. Therefore, the actual (management) IP address must be configured so that the FL MGUARD can establish the required connections.

The following are examples of how and why FL MGUARD communication takes place:
–   Communication with NTP servers to synchronize the time
–   Communication with DNS servers to resolve host names (especially those from VPN partners)
–   To register its IP address with a DynDNS service
–   To send SNMP traps
–   To forward log messages to a SysLog server
–   To download a CRL from an HTTP(S) server
–   To authenticate a user through a RADIUS server
–   To download a configuration profile through an HTTPS server
–   To download a firmware update from an HTTPS server

With firewall redundancy in Router network mode, devices connected to the same LAN segment as the redundant pair must use their respective virtual IP addresses as gateways for their routes. If these devices were to use the actual IP address of either of the FL MGUARD devices, this would work until that particular FL MGUARD failed. However, the other FL MGUARD would then not be able to take over.

Targets for the connectivity check

If a target is set for ICMP echo requests as part of the connectivity check, these requests must be answered within a certain time, even if the network is busy with other data. The network path between the redundant pair and these targets must be set so that it is also able to forward the ICMP responses when under heavy load. Otherwise, the connectivity check for an FL MGUARD could erroneously fail.

Targets can be configured for the internal and external interface in the connectivity check (see "Connectivity Checks" on page 278). It is important that these targets are actually connected to the specified interface. An ICMP echo reply cannot be received by an external interface when the target is connected to the internal interface (and vice versa). When the static routes are changed, it may easily happen to forget to adjust the configuration of the targets accordingly.

The targets for the connectivity check should be well thought out. Without a connectivity check, all it takes are two errors for a network lobotomy to occur.

A network lobotomy is prevented if the targets for both FL MGUARD devices are identical and all targets have to answer the request. However, the disadvantage of this method is that the connectivity check fails more often if one of the targets does not offer high availability.

In **Router network mode**, we recommend defining a highly available device as the target on the external interface. This can be the default gateway for the redundant pair (e.g., a virtual router comprised of two independent devices). In this case, either no targets or a selection of targets should be defined on the internal interface.

Please also note the following information when using a virtual router consisting of two independent devices as the default gateway for a redundant pair. If these devices use VRRP to synchronize their virtual IP, then a network lobotomy could split the virtual IP of this router into two identical copies. These routers could use a dynamic routing protocol and only one may be selected for the data flows of the network being monitored by the FL MGUARD. Only this router should keep the virtual IP. Otherwise, you can define targets which are accessible via this route in the connectivity check. In this case, the virtual IP address of the router would not be a sensible target.

Redundant group

Several redundant pairs can be connected within a LAN segment (redundant group). You define a value as an identifier (through the router ID) for each virtual instance of the redundant pair. As long as these identifiers are different, the redundant pairs do not come into conflict with each other.

Data traffic

In the event of a high **latency** in a network used for state synchronization updates or a serious data loss on this network, the FL MGUARD on standby is assigned the "outdated" state. This does not occur, however, as long as no more than two back-to-back updates are lost. This is because the FL MGUARD on standby automatically requests a repeat of the update. The latency requirements are the same as those detailed under"Fail-over switching time" on page 301.

Sufficient bandwidth

The data traffic generated as a result of the connectivity check, availability check, and state synchronization uses bandwidth on the network. The connectivity check also generates complicated calculations. There are several ways to limit this or stop it completely.

If the influence on other devices is unacceptable:

- – The connectivity check must either be deactivated, or must only relate to the actual IP address of the other FL MGUARD.
- – The data traffic generated by the availability check and state synchronization must be moved to a separate VLAN.
- – Switches must be used which allow separation of the VLANs.

X.509 certificates for SSH clients

The FL MGUARD supports the authentication of SSH clients using X.509 certificates. It is sufficient to configure CA certificates that are required for the establishment and validity check of a certificate chain. This certificate chain must exist between the CA certificate on the FL MGUARD and the X.509 certificate shown to the SSH client (see "Shell Access" on page 58).

If the validity period of the client certificate is checked by the FL MGUARD (see "Certificate settings" on page 169), new CA certificates must be configured on the FL MGUARD at some point. This must take place before the SSH clients use their new client certificates.

If the CRL check is activated (under *Authentication >> Certificates >> Certificate settings*), one URL (where the corresponding CRL is available) must be maintained for each CA certificate. The URL and CRL must be published before the FL MGUARD uses the CA certificates in order to confirm the validity of the certificates shown by the VPN partners.

6.1.9 Transmission capacity with firewall redundancy

These values apply to Router network mode when the data traffic for state synchronization is transmitted without encryption. If the transmission capacity described here is exceeded, in the event of errors the switching time may be longer than that set.

Platform	Transmission capacity with firewall redundancy
FL MGUARD RS4000	62 Mbps, bidirectional,
FL MGUARD SMART2	not more than 5250 frames/s
FL MGUARD PCI4000	
FL MGUARD DELTA TX/TX	

Fail-over switching time

The fail-over switching time can be set to 1, 3 or 10 seconds in the event of errors.

6.1.10   Limits of firewall redundancy

– In **Router network mode**, firewall redundancy is only supported with the "static" mode.
– Access to the FL MGUARD via the HTTPS, SNMP, and SSH **management protocols** is only possible with an actual IP address from each FL MGUARD. Access attempts to virtual addresses are rejected.
– The following **features cannot** be used with firewall redundancy.
    – A secondary external Ethernet interface
    – A DHCP server
    – A DHCP relay
    – A SEC-Stick server
    – A user firewall
    – CIFS Integrity Monitoring
– The redundant pair **must have the same configuration**. Take this into account when making the following settings:
    – NAT settings (masquerading, port forwarding, and 1:1 NAT)
    – Flood protection
    – Packet filter (firewall rules, MAC filter, advanced settings)
    – Queues and rules for QoS
– Some network connections may be interrupted following a **network lobotomy**. (See "Restoration in the event of a network lobotomy" on page 304)
– After a fail-over, **semi-unidirectional or complex connections** that were established in the second before the fail-over may be interrupted. (See "Fail-over when establishing complex connections" on page 304 and "Fail-over when establishing semi-unidirectional connections" on page 304.)
– State synchronization does not replicate the connection tracking entries for **ICMP echo requests** forwarded by the FL MGUARD. Therefore, ICMP echo replies can be dropped according to the firewall rules if they only reach the FL MGUARD after the fail-over is completed. Please note that ICMP echo replies are not suitable for measuring the fail-over switching time.
– **Masquerading** involves hiding the transmitter behind the first virtual IP address or the first internal IP address. This is different to masquerading on the FL MGUARD without firewall redundancy. When firewall redundancy is not activated, the external or internal IP address hiding the transmitter is specified in a routing table.

6.2　VPN redundancy

VPN redundancy can only be used together with firewall redundancy.

The concept is the same as for firewall redundancy. In order to detect an error in the system environment, the activity is transmitted from the active FL MGUARD to the FL MGUARD on standby.

At any given point in time, at least one FL MGUARD in the redundant pair is operating the VPN connection (except in the event of a network lobotomy).

Basic requirements for VPN redundancy

VPN redundancy does not have any of its own variables. It currently does not have its own menu in the user interface – it is activated together with firewall redundancy instead.

VPN redundancy can only be used if the corresponding license has been purchased and installed on the FL MGUARD.

As VPN connections must be established for VPN redundancy, a corresponding VPN license is also necessary.

If you only have the license for firewall redundancy and VPN connections are installed, VPN redundancy cannot be activated. An error message is displayed as soon as an attempt is made to use firewall redundancy.

Only identical FL MGUARD devices can be used together in a redundant pair.

6.2.1　Components in VPN redundancy

The components used in VPN redundancy are the same as described under firewall redundancy. One additional component is available here – VPN state synchronization. A small number of components are slightly expanded for VPN redundancy. However, the connectivity check, availability check, and firewall state synchronization are all performed in the same way as before.

VPN state synchronization

The FL MGUARD supports the configuration of firewall rules for the VPN connection.

VPN state synchronization monitors the state of the different VPN connections on the active FL MGUARD. It ensures that the FL MGUARD on standby receives a valid, up-to-date copy of the VPN state database.

As with state synchronization of the firewall, VPN state synchronization sends updates from the active FL MGUARD to the FL MGUARD on standby. If requested to do so by the FL MGUARD on standby, the active FL MGUARD sends a complete record of all state information.

Establishing VPN connections

In VPN redundancy, the virtual network interface is used for an additional purpose – to establish, accept, and operate the VPN connections. The FL MGUARD only listens on the first virtual IP address.

In Router network mode, the FL MGUARD listens at the first external and internal virtual IP addresses.

State monitoring

State monitoring is used to monitor state synchronization on both the VPN and firewall.

Status indicator

The status indicator shows additional detailed information on the status of VPN state synchronization. This is located directly next to the information for firewall state synchronization.

As an ancillary effect, the status indicator of the VPN connection can also be seen on the FL MGUARD on standby. You can, therefore, find the contents of the VPN state database replicated under the normal status indicator for the VPN connection (under *IPsec VPN >> IPsec Status*).

Only the state of the synchronization process is shown in the status indicator for firewall redundancy *(Redundancy >> FW Redundancy Status >> Redundancy Status)*.

6.2.2   Interaction of the VPN redundancy components

The individual components interact in the same way as described for firewall redundancy. VPN state synchronization is also controlled by state monitoring. The state is recorded and updates are sent.

Certain conditions must be met for the states to occur. VPN state synchronization is taken into account here.

6.2.3   Error compensation through VPN redundancy

VPN redundancy compensates for the exact same errors as firewall redundancy (see "Error compensation through firewall redundancy" on page 303).

However, the VPN section can hinder the other VPN gateways in the event of a network lobotomy. The independent FL MGUARD devices then have the same virtual IP address for communicating with the VPN partners. This can result in VPN connections being established and disconnected in quick succession.

6.2.4 Setting the variables for VPN redundancy

If the required license keys are installed, VPN redundancy is automatically activated at the same time as firewall redundancy. This occurs as soon as *Enable redundancy* is set to **Yes** in the *Redundancy >> Firewall Redundancy >> Redundancy* menu.

There is no separate menu for VPN redundancy. The existing firewall redundancy variables are expanded.

Table 6-3   Expanded functions with VPN redundancy activated

Redundancy >> Firewall Redundancy >> Redundancy		
General	**Enable redundancy**	Firewall redundancy and VPN redundancy are activated or deactivated.
Virtual interfaces	**External virtual IP addresses**	Only in Router network mode.
		The FL MGUARD uses the first external virtual IP address as the address from which it sends and receives IKE messages.
		The external virtual IP address is used instead of the actual primary IP address of the external network interface.
		The FL MGUARD no longer uses the actual IP address to send or answer IKE messages.
		ESP data traffic is handled similarly, but is also accepted and processed by the actual IP address.
	Internal virtual IP addresses	As described under *External virtual IP addresses* , but for internal virtual IP addresses.

6.2.5   Requirements for VPN redundancy

– VPN redundancy can only be activated if a **license key** is installed for VPN redundancy and a VPN connection is activated.

– **FL MGUARD RS4000 and FL MGUARD industrial rs only**

If a VPN connection is controlled via a **VPN switch**, then VPN redundancy cannot be activated.

(See under: *IPsec VPN >> Global >> Options >> VPN Switch*)

During VPN state synchronization, the state of the VPN connection is sent continuously from the active FL MGUARD to the FL MGUARD on standby so that it always has an up-to-date copy in the event of errors. The only exception is the state of the IPsec replay window. Changes there are only transmitted sporadically.

The volume of the data traffic for state synchronization does not depend on the data traffic sent over the VPN channels. The data volumes for state synchronization are defined by a range of parameters that are assigned to the ISAKMP SAs and IPsec SAs.

6.2.6   Handling VPN redundancy in extreme situations

The conditions listed under "Handling firewall redundancy in extreme situations" on page 304 also apply to VPN redundancy. They also apply when the FL MGUARD is used exclusively for forwarding VPN connections. The FL MGUARD forwards the data flows via the VPN channels and rejects incorrect packets, regardless of whether firewall rules have been defined for the VPN connections or not.

An error interrupts the flow of data traffic

An error that interrupts the data traffic running via the VPN channels represents an extreme situation. In this case, the IPsec data traffic is briefly vulnerable to replay attacks. (A replay attack is the repetition of previously sent encrypted data packets using copies which have been saved by the attacker.) The data traffic is protected by sequential numbers. Independent sequential numbers are used for each direction in an IPsec channel. The FL MGUARD drops ESP packets which have the same sequential number as a packet that has already been decrypted for a specific IPsec channel by the FL MGUARD. This mechanism is known as the **IPsec replay window**.

The IPsec replay window is only replicated sporadically during state synchronization, as it is very resource-intensive. Therefore, the active FL MGUARD may have an obsolete IPsec replay window following a fail-over. An attack is then possible until the real VPN partner has sent the next ESP packet for the corresponding IPsec SA, or until the IPsec SA has been renewed.

To avoid having an insufficient sequential number for the outgoing IPsec SA, VPN redundancy adds a constant value to the sequential number for each outgoing IPsec SA before the FL MGUARD becomes active. This value is calculated so that it corresponds to the maximum number of data packets which can be sent through the VPN channel during the maximum fail-over switching time. In the worst case (1 Gigabit Ethernet and a switching time of 10 seconds), this is 0.5% of an IPsec sequence. At best, this is only a per thousand value.

Adding a constant value to the sequential number prevents the accidental reuse of a sequence number already used by the other FL MGUARD shortly before it failed. Another effect is that ESP packets sent from the previously active FL MGUARD are dropped by the VPN partner if new ESP packets are received earlier from the FL MGUARD that is currently active. To do this, the latency on the network must differ from the fail-over switching time.

An error interrupts the initial establishment of the ISAKMP SA or IPsec SA

If an error interrupts the initial establishment of the ISAKMP SA or IPsec SA, the FL MGUARD on standby can continue the process seamlessly, as the state of the SA is replicated synchronously. The response to an IKE message is only sent from the active FL MGUARD after the FL MGUARD on standby has confirmed receipt of the corresponding VPN state synchronization update.

When an FL MGUARD becomes active, it immediately repeats the last IKE message which should have been sent from the previously active FL MGUARD. This compensates for cases where the previously active FL MGUARD has sent the state synchronization but has failed before it could send the corresponding IKE message.

In this way, the establishment of the ISAKMP SA or IPsec SA is only delayed by the switching time during a fail-over.

An error interrupts the renewal of an ISAKMP SA

If an error interrupts the renewal of an ISAKMP SA, this is compensated in the same way as during the initial establishment of the SA. The old ISAKMP SA is also kept for Dead Peer Detection until the renewal of the ISAKMP SA is complete.

An error interrupts the renewal of an IPsec SA

If an error interrupts the renewal of an IPsec SA, this is compensated in the same way as during the initial establishment of the SA. Until renewal of the ISAKMP SA is complete, the old outgoing and incoming IPsec SAs are retained until the VPN partner notices the change.

VPN state synchronization ensures that the old IPsec SAs are retained throughout the entire time that the FL MGUARD remains on standby. When the FL MGUARD becomes active, it can then continue with the encryption and decryption of the data traffic without the need for further action.

Loss of data packets during VPN state synchronization

State synchronization can cope with the loss of one of two back-to-back update packets. If more data packets are lost, this can result in a longer switching time in the event of errors.

The FL MGUARD on standby has an obsolete machine certificate

X.509 certificates and private keys used by a redundant pair to authenticate itself as a VPN partner may need to be changed. The combination of a private key and certificate is hereafter referred to as a machine certificate.

Each FL MGUARD in a redundant pair must be reconfigured in order to switch the machine certificate. Both FL MGUARD devices also require the same certificate so that their VPN partners view them as one and the same virtual VPN device.

As each FL MGUARD has to be reconfigured individually, it may be the case that the FL MGUARD on standby has an obsolete machine certificate for a brief period.

If the FL MGUARD on standby becomes active at the exact moment when the ISAKMP SAs are being established, this procedure cannot be continued with an obsolete machine certificate.

As a countermeasure, VPN state synchronization replicates the machine certificate from the active FL MGUARD to the FL MGUARD on standby. In the event of a fail-over, the FL MGUARD on standby will only use this to complete the process of establishing the ISAKMP SAs where this has already been started.

If the FL MGUARD on standby establishes new ISAKMP SAs after a fail-over, it uses the machine certificate that has already been configured.

VPN state synchronization therefore ensures that the currently used machine certificates are replicated. However, it does not replicate the configuration itself.

The FL MGUARD on standby has an obsolete Pre-Shared Key (PSK)

Pre-Shared Keys (PSK) also need to be renewed on occasion in order to authenticate VPN partners. The redundant FL MGUARD devices may then have a different PSK for a brief period. In this case, only one of the FL MGUARD devices can establish a VPN connection as most VPN partners only accept one PSK. The FL MGUARD does not offer any countermeasures for this.

i	We therefore recommend using X.509 certificates instead of PSKs.

If VPN state synchronization replicates the PSKs being sent to the FL MGUARD on standby for a prolonged period, an incorrect configuration remains concealed during this period, making it difficult to detect.

6.2.7   Interaction with other devices

Resolving host names

If host names are configured as VPN gateways, the FL MGUARD devices in a redundant pair must be able to resolve the host names for the same IP address. This applies especially when *DynDNS Monitoring* (see *Page 221*) is activated.

If the host names are resolved from the FL MGUARD on standby to another IP address, the VPN connection to this host is interrupted following a fail-over. The VPN connection is reestablished through another IP address. This takes place directly after the fail-over. However, a short delay may occur, depending (among other things) on what value is entered under *DynDNS Monitoring* for the *Refresh Interval (sec)* .

Obsolete IPsec replay window

IPsec data traffic is protected against unauthorized access. To this end, each IPsec channel is assigned an independent sequential number. The FL MGUARD drops ESP packets which have the same sequential number as a packet that has already been decrypted for a specific IPsec channel by the FL MGUARD. This mechanism is known as the **IPsec replay window**. It prevents replay attacks, where an attacker sends previously recorded data to simulate someone else's identity.

The IPsec replay window is only replicated sporadically during state synchronization, as it is very resource-intensive. Therefore, the active FL MGUARD may have an obsolete IPsec replay window following a fail-over. This means that a replay attack is possible for a brief period until the real VPN partner has sent the next ESP packet for the corresponding IPsec SA, or until the IPsec SA has been renewed. However, the traffic must be captured completely for this to occur.

Dead Peer Detection

Please note the following point for Dead Peer Detection.

	With Dead Peer Detection, set a higher timeout than the upper limit for the *Fail-over switching time* on the redundant pair.
	(See under: *IPsec VPN >> Connections >> Edit >> IKE Options , Delay between requests for a sign of life*)

Otherwise, the VPN partners may think that the redundant pair is dead, even though it is only dealing with a fail-over.

Data traffic

In the event of a high latency in a network used for state synchronization updates, the FL MGUARD on standby is assigned the "outdated" state. The same thing also happens in the event of serious data losses on this network.

This does not occur, however, as long as no more than two back-to-back updates are lost. This is because the FL MGUARD on standby automatically requests a repeat of the update. The latency requirements are the same as those detailed under"Fail-over switching time" on page 301.

Actual IP addresses

VPN partners may not send ESP traffic to the actual IP address of the redundant pair. VPN partners must always use the virtual IP address of the redundant pair to send IKE messages or ESP traffic.

6.2.8   Transmission capacity with VPN redundancy

These values apply to Router network mode when the data traffic for state synchronization is transmitted without encryption. If the transmission capacity described here is exceeded, in the event of errors the switching time may be longer than that set.

Platform	Transmission capacity with firewall redundancy
FL MGUARD RS4000	17 Mbps, bidirectional,
FL MGUARD SMART2	not more than 2300 frames/s
FL MGUARD PCI4000	
FL MGUARD DELTA TX/TX	

Fail-over switching time

The fail-over switching time can be set to 1, 3 or 10 seconds in the event of errors.

6.2.9   Limits of VPN redundancy

The limits documented above for firewall redundancy also apply to VPN redundancy (see "Limits of firewall redundancy" on page 310). Further restrictions also apply.

–   The redundant pair must **have the same configuration** with respect to the following:
    –   General VPN settings
    –   Each individual VPN connection
–   The FL MGUARD only accepts VPN connections on the **first virtual IP address**.
    –   In Router network mode, this means the first internal IP address and the first external IP address.
–   The following **features cannot** be used with VPN redundancy:
    –   Dynamic activation of the VPN connections using a VPN switch or the CGI script command nph-vpn.cgi (only on FL MGUARD RS4000/RS2000 and FL MGUARD industrial rs)
    –   Archiving of diagnostic messages for VPN connections
–   VPN connections are only supported in Tunnel mode. Transport mode does not take sufficient account of VPN connections.
–   The upper limit of the **fail-over switching time** does not apply to connections which are **encapsulated with TCP**. Connections of this type are interrupted for a prolonged period during a fail-over. The encapsulated TCP connections must be reestablished by the initiating side after each fail-over. If the fail-over occurred on the initiating side, they can start immediately after the transfer. However, if the fail-over occurred on the answering side, the initiator must first detect the interruption and then reestablish the connection.
–   VPN redundancy supports **masquerading** in the same way as without VPN redundancy. This applies when a redundant pair is masked by a NAT gateway with a dynamic IP address.

    For example, a redundant pair can be hidden behind a DSL router, which masks the redundant pair with an official IP address. This DSL router forwards the IPsec data traffic (IKE and ESP, UDP ports 500 and 4500) to the virtual IP addresses. If the dynamic IP address changes, all active VPN connections which run via the NAT gateway are reestablished.

    The connections are reestablished by means of Dead Peer Detection (DPD) using the relevant configured time. This effect is beyond the influence of the FL MGUARD.
–   The redundancy function on the FL MGUARD does not support **path redundancy**. Path redundancy can be achieved using other methods, e.g., by using a router pair. This router pair is seen on the virtual side of the FL MGUARD devices. By contrast, on the other side, each of the routers has different connections.

    Path redundancy must not use NAT mechanisms such as masquerading to hide the virtual IP addresses of the FL MGUARD devices. Otherwise, a migration from one path to another would change the IP addresses used to mask the redundant pair. This would mean that all VPN connections (all ISAKMP SAs and all IPsec SAs) would have to be reestablished.

    The connections are reestablished by means of Dead Peer Detection (DPD) using the relevant configured time. This effect is beyond the influence of the FL MGUARD.
–   In the event of path redundancy caused by a network lobotomy, the VPN connections are no longer supported. A network lobotomy must be prevented whenever possible.

X.509 certificates for VPN authentication

The FL MGUARD supports the use of X.509 certificates when establishing VPN connections. This is described in detail under "Authentication" on page 237.

However, there are some special points to note when X.509 certificates are used for authenticating VPN connections in conjunction with firewall redundancy and VPN redundancy.

Switching machine certificates

A redundant pair can be configured so that it uses an X.509 certificate and the corresponding private key together to identify itself to a remote VPN partner as an individual virtual VPN instance.

These X.509 certificates must be renewed regularly. If the VPN partner is set to check the validity period of the certificates, these certificates must be renewed before their validity expires (see "Certificate settings" on page 169).

If a machine certificate is replaced, all VPN connections which use it are restarted by the FL MGUARD. While this is taking place, the FL MGUARD cannot forward any data via the affected VPN connections for a certain period of time. This period depends on the number of VPN connections affected, the performance of the FL MGUARD and VPN partners, and the latency of the FL MGUARD devices on the network.

If this is not feasible for redundancy, the VPN partners of a redundant pair must be configured so that they accept all certificates whose validity is confirmed by a set of specific CA certificates (see "CA certificates" on page 173 and "Authentication" on page 237).

> To do this, select **Signed by any trusted CA** under *IPsec VPN >> Connections >> Edit >> Authentication* / *Remote CA Certificate* .

If the new machine certificate is issued from a different sub-CA certificate, the VPN partner must be able to recognize this before the redundant pair can use the new machine certificate.

The machine certificate must be replaced on both FL MGUARD devices in a redundant pair. However, this is not always possible if one cannot be reached. This might be the case in the event of a network failure, for example. The FL MGUARD on standby may then have an obsolete machine certificate when it becomes active. This is another reason for setting the VPN partners so that they use both machine certificates.

The machine certificate is normally also replicated with the corresponding key during VPN state synchronization. In the event of a fail-over, the other FL MGUARD can take over and even continue establishing incomplete ISAKMP SAs.

Switching the remote certificates for a VPN connection

The FL MGUARD can be set to authenticate VPN partners directly using the X.509 certificates shown by these VPN partners. For this to happen, the relevant X.509 certificate must be set on the FL MGUARD. This is known as the *Remote CA Certificate* .

If a remote certificate is renewed, for a brief period, only one of the FL MGUARD devices will have a new certificate. We therefore recommend authenticating the VPN partners using CA certificates instead of remote certificates in VPN redundancy.

Adding a new CA certificate to identify VPN partners

The FL MGUARD can be set to authenticate VPN partners using CA certificates (see "CA certificates" on page 173 and "Authentication" on page 237).

To do this, select **Signed by any trusted CA** under *IPsec VPN >> Connections >> Edit >> Authentication / Remote CA Certificate* .

With this setting, a new CA certificate can be added without affecting the established VPN connections. However, the new CA certificates are used immediately. The X.509 certificate used by the VPN partner to authenticate itself to the FL MGUARD can then be replaced with minimal interruption. The only requirement is ensuring that the new CA certificate is available first.

The FL MGUARD can be set to check the validity period of the certificates provided by the VPN partner (see "Certificate settings" on page 169). In this case, new trusted CA certificates must be added to the FL MGUARD configuration. These certificates should also have a validity period.

If the CRL check is activated (under *Authentication >> Certificates >> Certificate settings*), one URL (where the corresponding CRL is available) must be maintained for each CA certificate. The URL and CRL must be published before the FL MGUARD uses the CA certificates in order to confirm the validity of the certificates shown by the VPN partners.

Using X.509 certificates with limited validity periods and CRL checks

The use of X.509 certificates is described under "Certificate settings" on page 169 (*Authentication >> Certificates >> Certificate settings* menu).

If X.509 certificates are used and **Check the validity period of certificates and CRLs** is set, the system time has to be correct. We recommend synchronizing the system time using a trusted **NTP server**. Each FL MGUARD in a redundant pair can use the other as an additional NTP server, but not as the only NTP server.

Product designation

7 NOTE: Restart, recovery procedure, and flashing the firmware

The **Rescue button** or **Reset button** is used to perform the following procedures on the devices shown in Figure 7-1:
– Performing a restart
– Performing a recovery procedure
– Flashing the firmware/rescue procedure
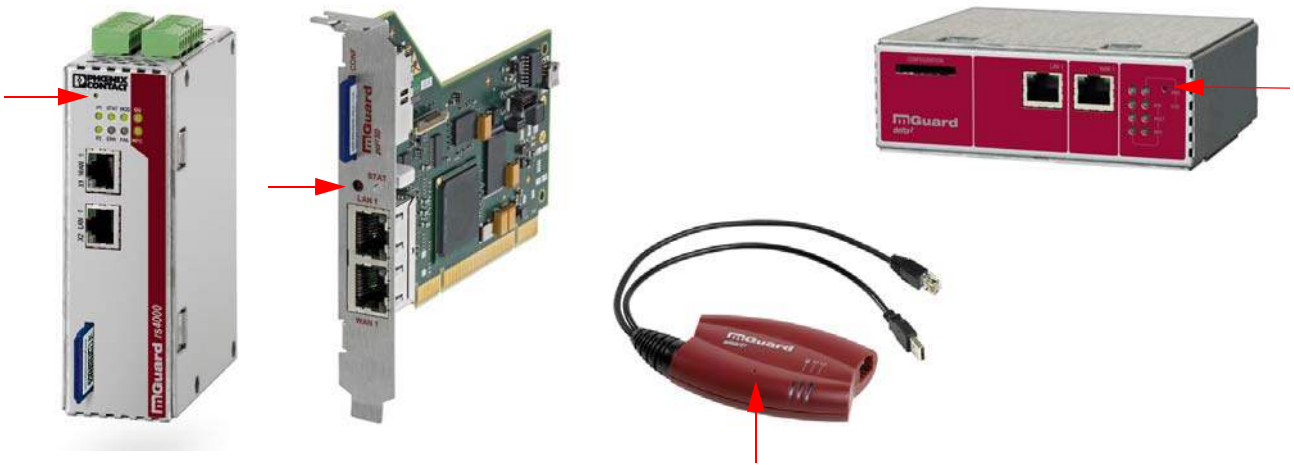
Figure 7-1   Rescue button

7.1   Performing a restart

Aim

The device is restarted with the configured settings.

Action

FL MGUARD PCI4000: Press the Reset button until the STAT LED lights up orange.

Press the Rescue button on the other FL MGUARD devices for around 1.5 seconds.
• **FL MGUARD RS4000/RS2000,** FL MGUARD DELTA TX/TX: Until the ERR LED lights up
• **FL MGUARD SMART2**: Until the middle LED lights up red

Alternatively:
• Temporarily disconnect the power supply.
• **FL MGUARD PCI4000**: Restart the computer that contains the FL MGUARD PCI4000 card.

7.2 Performing a recovery procedure

Aim

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 FL MGUARD.

When performing the recovery procedure, the default settings are established for all FL MGUARD models according to the following table:

Table 7-1 Preset addresses

Default settings	Network mode	Management IP #1	Management IP #2
FL MGUARD RS4000/RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

– The following applies to FL MGUARD models that are reset to *Stealth* mode (with the "multiple clients" default settings):
– 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 FL MGUARD is in Router or PPPoE mode.
– The configured device address of the FL MGUARD differs from the default setting.
– The current IP address of the device is not known.

i	Up-to-date information on the recovery and flashing procedure can be found in the application note for your FL MGUARD firmware version. (Application notes are available in the download area at innominate.com.)

FL MGUARD RS4000/RS2000, FL MGUARD SMART2, FL MGUARD PCI4000 , FL MGUARD DELTA TX/TX:

• Slowly press the **Rescue**/**Reset button** six times.

The FL MGUARD responds after around two seconds:

FL MGUARD RS4000/ RS2000, FL MGUARD PCI4000, FL MGUARD DELTA TX/TX	The STAT LED lights up green.

- Slowly press the **Rescue**/**Reset button** again six times.

FL MGUARD RS4000/RS2000, FL MGUARD DELTA TX/TX	If successful, the STAT LED lights up green. If unsuccessful, the ERR LED lights up red.
FL MGUARD PCI4000	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* or *Router* mode. The device can then be reached again at the corresponding addresses, see Table "Preset addresses" on page 324.

7.3 Flashing the firmware/rescue procedure

Aim

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

– **All configured settings are deleted.** The FL MGUARD is set to the delivery state.
– In Version 5.0.0 or later of the FL MGUARD, the licenses installed on the FL MGUARD are retained after flashing the firmware. Therefore, they do not have to be installed again.
– Only firmware Version 5.1.0 or later can be installed on the FL MGUARD industrial rs.

Possible reasons:

– The administrator and root password have been lost.

Requirements

7.3.1 Requirements for flashing

Requirements for the DHCP and TFTP server

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 329).

No such server is required for the **FL MGUARD RS4000/RS2000, FL MGUARD PCI4000 and FL MGUARD DELTA TX/TX** if the firmware is to be loaded from an SD card. 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).

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

– The FL MGUARD firmware has been saved on the configuration computer.
– DHCP and TFTP servers can be accessed under the same IP address.
– **FL MGUARD RS4000/RS2000, FL MGUARD PCI4000 and FL MGUARD DELTA TX/TX**:
   – The FL MGUARD firmware has been obtained from your dealer's support team or the innominate.com website and has been saved on a compatible SD card.
   – This SD card has been inserted into the FL MGUARD.

The relevant firmware files are available for download from the download page of innominate.com. 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

– **FL MGUARD PCI4000**: If the FL MGUARD is operated in **Power over PCI mode**, the DHCP/TFTP server must be connected via the LAN socket of the FL MGUARD.

Action

7.3.2 Flashing procedure for FL MGUARD RS4000/RS2000, FL MGUARD SMART2, FL MGUARD DELTA TX/TX

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

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

• Press and hold down the **Rescue button** until the device enters *recovery status*:

The FL MGUARD is restarted (after around 1.5 seconds); after a further 1.5 seconds, the FL MGUARD enters *recovery status*:

The reaction of the device depends on its type:

FL MGUARD RS4000/ RS2000, FL MGUARD DELTA TX/TX	The STAT, MOD and SIG LEDs light up green.

Release the **Rescue button within a second of entering** *recovery status*.

(If the **Rescue button** is not released, the FL MGUARD is restarted.)

The FL MGUARD now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

The reaction of the device depends on its type:

FL MGUARD RS4000/ RS2000, FL MGUARD DELTA TX/TX	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 signed by Innominate are executed.

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

The reaction of the device depends on its type:

FL MGUARD RS4000/ RS2000, FL MGUARD DELTA TX/TX	The STAT, MOD, and SIG LEDs form a light sequence.

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 FL MGUARD operating system and is signed electronically. Only files signed by Innominate are accepted.

This process takes around 3 to 5 minutes.

The reaction of the device depends on its type:

FL MGUARD RS4000/ RS2000, FL MGUARD DELTA TX/TX	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 has been completed, the following occurs:

FL MGUARD RS4000/ RS2000, FL MGUARD DELTA TX/TX	The STAT, MOD", and SIG" LEDs flash green simultaneously.

- Restart the FL MGUARD. This is not necessary for the FL MGUARD blade and FL MGUARD PCI4000.
- To do this, briefly press the **Rescue button**.

    (Alternatively, you can disconnect and reconnect the power supply. On the FL MGUARD SMART2, you can disconnect and insert the USB cable as it is only used for the power supply.)

The FL MGUARD is in the delivery state. You can now configure it again (see "Establishing a local configuration connection" on page 43):

After the restart, the **FL MGUARD PCI4000** is automatically assigned a management IP address. This address is assigned by a BootP server that can be accessed on the network and was used during flashing.

If the recommended DHCP server is also used for Windows (see Page 329), it also operates as the BootP server. This does not apply when using a DHCP server under Linux.

7.3.3   Flashing procedure for the FL MGUARD PCI4000

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).
– This SD card has been inserted into the FL MGUARD.
– The relevant firmware files are available for download from the download page of innominate.com. 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 upper two LEDs of the Ethernet sockets light up green one after the other.
• Release the Reset button during the green light phase.
   The flashing procedure is started.

7.3.4 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 innominate.com.
- 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 FL 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**.

  Make sure that this is the correct license file for the device (see "Management >> Update" on page 82).
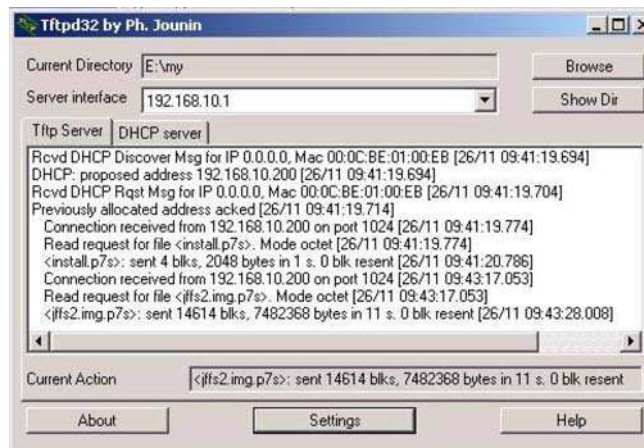
Figure 7-2   Entering the host IP

- Switch to the "TFTP Server" or "DHCP Server" tab page and click on "Settings" to set the parameters as follows:
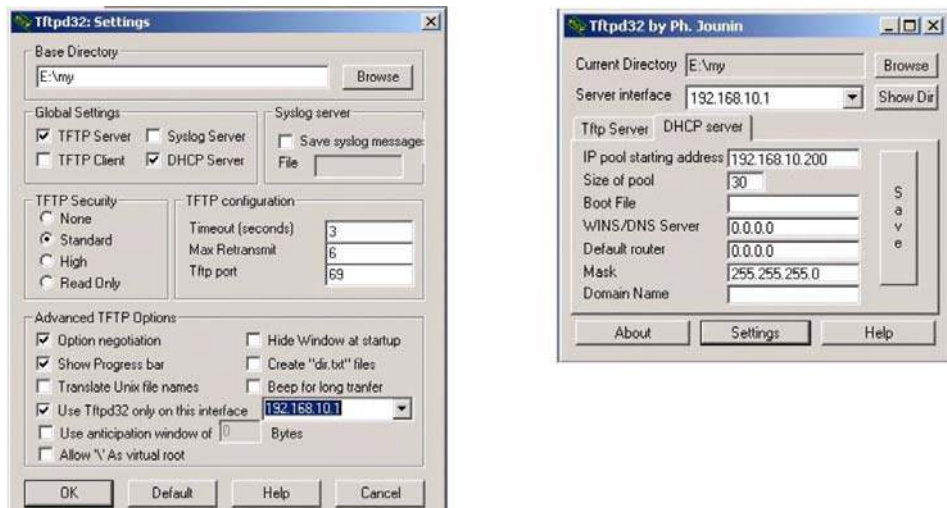
Figure 7-3   Settings

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 FL 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 (see "Management >> Update" on page 82).

- 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.

8   Technical data

8.1   FL MGUARD RS4000/RS2000

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 ǀ 1 WAN port Ethernet IEEE 802.3 10/100 Base TX RJ45 ǀ full duplex ǀ auto MDIX	1 LAN port ǀ 1 WAN port Ethernet IEEE 802.3 10/100 Base TX RJ45 ǀ full duplex ǀ auto MDIX
Other interfaces	Serial RS-232 D-SUB 9 connector 2 digital inputs and 2 digital outputs	Serial RS-232 D-SUB 9 connector 2 digital inputs and 2 digital outputs
Memory	128 MB RAM ǀ 128 MB Flash SD card Replaceable configuration memory	128 MB RAM ǀ 128 MB Flash SD card Replaceable configuration memory
High availability	Optional: VPN ǀ 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 (W x H 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)	722 g (TX/TX)

Firmware and power values		
Firmware compatibility	FL 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 (router ǀ firewall)	- Router mode, default firewall rules, bidirectional throughput: max. 124 Mbps - Stealth mode, default firewall rules, bidirectional throughput max. 58 Mbps	- Router mode, default firewall rules, bidirectional throughput: max. 124 Mbps - Stealth mode, default firewall rules, bidirectional throughput max. 58 Mbps
Virtual Private Network (VPN)	IPsec (IETF standard) Up to 250 VPN tunnels	IPsec (IETF standard) Up to 2 VPN tunnels
Hardware-based encryption	DES ǀ 3DES ǀ AES-128/192/256	DES ǀ 3DES ǀ AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: max. 40 Mbps Stealth mode, default firewall rules, bidirectional throughput max. 26 Mbps	Router mode, default firewall rules, bidirectional throughput: max. 40 Mbps Stealth mode, default firewall rules, bidirectional throughput max. 26 Mbps
Management support	Web GUI (HTTPS) ǀ command line interface (SSH) ǀ SNMP v1/2/3 ǀ central device management software	
Diagnostics	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) signal contacts ǀ service contacts ǀ log file ǀ remote syslog	LEDs (Power, State, Error, Signal, Fault, Modem, Info) signal contacts ǀ service contacts ǀ log file ǀ remote syslog

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

8.2   FL MGUARD PCI4000

FL MGUARD PCI4000 ǀ FL MGUARD PCI4000e

Hardware properties	
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port ǀ 1 WAN port
	Ethernet IEEE 802.3 10/100 Base TX ǀ
	RJ45 ǀ full duplex ǀ auto MDIX
Other interfaces	Serial RS-232, internal connector
Memory	128 MB RAM ǀ 128 MB Flash SD card ǀ replaceable configuration memory
Drives	–
High availability	Optional: VPN ǀ router
Power supply	3.3 V or 5 V
	Via PCI- (FL MGUARD PCI4000) or PCI Express bus (FL MGUARD PCI4000e)
Power consumption	3.7 W ... 4.2 W, typical
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	0°C ... +70°C (operation)
	-20°C ... +70°C (storage)
With battery	0°C ... +60°C (operation)
	-20°C ... +60°C (storage)
Dimensions (W x H x D)	950 mm x 18 mm x 130 mm
Weight	72 g

Firmware and power values	
Firmware compatibility	FL MGUARD v7.5.0 or later; Innominate 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 (router ǀ firewall)	- Router mode, default firewall rules, bidirectional throughput: max. 124 Mbps - Stealth mode, default firewall rules, bidirectional throughput max. 58 Mbps
Hardware-based encryption	DES ǀ 3DES ǀ AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: max. 40 Mbps Stealth mode, default firewall rules, bidirectional throughput max. 26 Mbps
Management support	Web GUI (HTTPS) ǀ command line interface (SSH) ǀ SNMP v1/2/3 ǀ 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) ǀ log file ǀ remote-syslog

Other	
Conformity	CE	FCC
Special features	Realtime clock	Trusted Platform Module (TPM)	temperature sensor	FL MGUARD Remote Services Portal ready

8.3 FL MGUARD DELTA TX/TX

Hardware properties

Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port | 1 WAN port Ethernet IEEE 802.3 10/100 Base TX | RJ45 | full duplex | auto MDIX
Other interfaces	Serial RS-232, D-SUB 9 connector
Memory	128 MB RAM | 128 MB Flash SD card, replaceable configuration memory
High availability	Optional: VPN | router
Power supply	External power supply unit 12 V / 0.85A DC | 100 – 240 V / 0.4A 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 (W x H x D)	45 x 130 x 114 mm
Weight	629 g

Firmware and power values

Firmware compatibility	FL 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 (router | firewall)	- Router mode, default firewall rules, bidirectional throughput: max. 124 Mbps - Stealth mode, default firewall rules, bidirectional throughput max. 58 Mbps
Virtual Private Network (VPN)	IPsec (IETF standard), VPN models up to 10 tunnels, up to 250 as an option
Hardware-based encryption	DES | 3DES | AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: max. 40 Mbps Stealth mode, default firewall rules, bidirectional throughput max. 26 Mbps
Management support	Web GUI (HTTPS) | command line interface (SSH) | SNMP v1/2/3 | central device management software
Diagnostics	LEDs (Power, State, Error, Signal, Fault, Modem, Info) | log file | remote syslog

Other

Conformity	CE | FCC
Special features	Realtime clock | Trusted Platform Module (TPM) | temperature sensor | FL MGUARD Remote Services Portal ready

8.4   FL MGUARD SMART2

Hardware properties	
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 cnnection
Drives	–
High availability	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 (W x H x D)	27 x 77 x 115 mm
Weight	131 g

Firmware and power values	
Firmware compatibility	FL MGUARD v7.2 or later; Phoenix Contact recommends using firmware version 7.x with the respective current patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	- Router mode, default firewall rules, bidirectional throughput: max. 124 Mbps - Stealth mode, default firewall rules, bidirectional throughput max. 58 Mbps
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: max. 40 Mbps Stealth mode, default firewall rules, bidirectional throughput max. 26 Mbps
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (3 LEDs in combination for boot process, heartbeat, system error, Ethernet status, recovery mode) I log file I remote syslog

Other	
Conformity	CE I FCC
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor

8.5 Ordering data

8.5.1 Products

Description	Order designation	Order No.	Pcs. / Pkt.
Security device in metal housing, with extended temperature range, SD card slot, up to 2 VPN tunnels, 2-click firewall for maximum ease of configuration, router with NAT/1:1 NAT	FL MGUARD RS2000 TX/TX VPN	2700642	1
Security device in metal housing, with extended temperature range, SD card slot, intelligent firewall with full scope of functions for maximum security and ease of configuration, router with NAT/1:1 NAT, optional VPN/CIFS integrity monitoring	FL MGUARD RS4000 TX/TX	2700634	1
Security device in metal housing, with extended temperature range, SD card slot, VPN, intelligent firewall with full scope of functions for maximum security and ease of configuration, router with NAT/1:1 NAT, optional CIFS integrity monitoring	FL MGUARD RS4000 TX/TX VPN	2200515	1
Router with intelligent firewall, stateful inspection firewall for maximum security and ease of configuration	FL MGUARD SMART2	2700640	1
Router with intelligent firewall, stateful inspection firewall for maximum security and ease of configuration, VPN according to IPsec standard, hardware encryption with up to 35 Mbps	FL MGUARD SMART2 VPN	2700639	1
Security device in metal housing, SD card slot, intelligent firewall with full scope of functions for maximum security and ease of configuration, router with NAT/1:1 NAT, optional VPN/CIFS integrity monitoring	FL MGUARD DELTA TX/TX	2700967	1
Security device in PCI format, SD card slot, intelligent firewall with full scope of functions for maximum security and ease of configuration, router with NAT/1:1 NAT, optional VPN/CIFS integrity monitoring	FL MGUARD MGUARD PCI4000	2701274	1
Security device in PCI format, SD card slot, intelligent firewall with full scope of functions for maximum security and ease of configuration, router with NAT/1:1 NAT, VPN, optional CIFS integrity monitoring	FL MGUARD MGUARD PCI4000	2701275	1

8.5.2 Accessories

Description	Order designation	Order No.	Pcs. / Pkt.
Universal end clamp	E/NS 35 N	0800886	1
SD card, 256 MB	SD FLASH, 256 MB	2988120	1
SD card, 512 MB	SD FLASH, 512 MB	2988146	1
Network monitoring with HMI/SCADA systems	FL SMNP OPC SERVER V3	2701139	1
Patch cable, CAT6, pre-assembled, 0.3 m long	FL CAT6 PATCH 0,3	2891181	10
Patch cable, CAT6, pre-assembled, 0.5 m long	FL CAT6 PATCH 0,5	2891288	10
Patch cable, CAT6, pre-assembled, 1.0 m long	FL CAT6 PATCH 1,0	2891385	10
Patch cable, CAT6, pre-assembled, 1.5 m long	FL CAT6 PATCH 1,5	2891482	10
Patch cable, CAT6, pre-assembled, 2.0 m long	FL CAT6 PATCH 2,0	2891589	10
Patch cable, CAT6, pre-assembled, 3.0 m long	FL CAT6 PATCH 3,0	2891686	10
Patch cable, CAT6, pre-assembled, 5.0 m long	FL CAT6 PATCH 5,0	2891783	10
Patch cable, CAT6, pre-assembled, 7.5 m long	FL CAT6 PATCH 7,5	2891880	10
Patch cable, CAT6, pre-assembled, 10 m long	FL CAT6 PATCH 10	2891887	10
Patch cable, CAT6, pre-assembled, 12.5 m long	FL CAT6 PATCH 12,5	2891369	5
Patch cable, CAT6, pre-assembled, 15 m long	FL CAT6 PATCH 15	2891372	5
Patch cable, CAT6, pre-assembled, 20 m long	FL CAT6 PATCH 20	2891576	5

Description [...]	Order designation	Order No.	Pcs. / Pkt.
Patch cable, CAT5, pre-assembled, 0.3 m long	FL CAT5 PATCH 0,3	2832250	10
Patch cable, CAT5, pre-assembled, 0.5 m long	FL CAT5 PATCH 0,5	2832263	10
Patch cable, CAT5, pre-assembled, 1.0 m long	FL CAT5 PATCH 1,0	2832276	10
Patch cable, CAT5, pre-assembled, 1.5 m long	FL CAT5 PATCH 1,5	2832221	10
Patch cable, CAT5, pre-assembled, 2.0 m long	FL CAT5 PATCH 2,0	2832289	10
Patch cable, CAT5, pre-assembled, 3.0 m long	FL CAT5 PATCH 3,0	2832292	10
Patch cable, CAT5, pre-assembled, 5.0 m long	FL CAT5 PATCH 5,0	2832580	10
Patch cable, CAT5, pre-assembled, 7.5 m long	FL CAT5 PATCH 7,5	2832616	10
Patch cable, CAT5, pre-assembled, 10.0 m long	FL CAT5 PATCH 10	2832629	10
Color coding for FL CAT5/6 PATCH ..., black	FL PATCH CCODE BK	2891194	20
Color coding for FL CAT5/6 PATCH ..., brown	FL PATCH CCODE BN	2891495	20
Color coding for FL CAT5/6 PATCH ..., blue	FL PATCH CCODE BU	2891291	20
Color coding for FL CAT5/6 PATCH ..., green	FL PATCH CCODE GN	2891796	20
Color coding for FL CAT5/6 PATCH ..., gray	FL PATCH CCODE GY	2891699	20
Color coding for FL CAT5/6 PATCH ..., red	FL PATCH CCODE RD	2891893	20
Color coding for FL CAT5/6 PATCH ..., violet	FL PATCH CCODE VT	2891990	20
Color coding for FL CAT5/6 PATCH ..., yellow	FL PATCH CCODE YE	2891592	20
Lockable security element for FL CAT5/6 PATCH ...	FL PATCH GUARD	2891424	20
Color coding for FL PATCH GUARD, black	FL PATCH GUARD CCODE BK	2891136	12
Color coding for FL PATCH GUARD, blue	FL PATCH GUARD CCODE BUFL PATCH GUARD CCODE BU	2891233	12
Color coding for FL PATCH GUARD, green	FL PATCH GUARD CCODE GN	2891631	12
Color coding for FL PATCH GUARD, orange	FL PATCH GUARD CCODE OG	2891330	12
Color coding for FL PATCH GUARD, red	FL PATCH GUARD CCODE RD	2891738	12
Color coding for FL PATCH GUARD, turquoise	FL PATCH GUARD CCODE TQ	2891534	12
Color coding for FL PATCH GUARD, violet	FL PATCH GUARD CCODE VT	2891835	12
Color coding for FL PATCH GUARD, yellow	FL PATCH GUARD CCODE YE	2891437	12
Key for FL PATCH GUARD	FL PATCH GUARD KEY	2891521	1
Security element for FL CAT5/6 PATCH ...	FL PATCH SAFE CLIP	2891246	20

HOTLINE:

If there are any problems that cannot be solved using this documentation, please call our hotline: + 49 (0) 52 81 - 946 28 88