AUTOMATION

User manual

UM EN FL MGUARD

Order No.: -

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

PHOENIX CONTACT
INSPIRING INNOVATIONS

AUTOMATION

User manual

FL MGUARD

Software release 7.2.0

2012-05-30

Designation: UM EN FL MGUARD

Revision: 04

Order No.: —

This user manual is valid for the FL MGUARD software release 7.2.0
when using devices of the FL MGUARD product range:

Please observe the following notes

In order to ensure the safe use of the product described, you have to read and understand this manual. The following notes provide information on how to use this user manual.

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 relevant safety concepts of automation technology as well as applicable standards and other regulations.

Phoenix Contact accepts no liability for erroneous handling or damage to products from Phoenix Contact or third-party products resulting from disregard of information contained in this user manual.

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.

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.

The following types of message provide information about possible property damage and general information concerning proper operation and ease of use.

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

This symbol and the accompanying text provide the reader with additional information, such as tips and advice on the efficient use of hardware and on software optimization. It is also used as a reference to other sources of information (user manuals, data sheets).

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 data sheets, installation instructions, user manuals, etc.) does not constitute any further duty on the part of Phoenix Contact to furnish information on alterations to products and/or technical documentation. Any other agreement shall only apply if expressly confirmed in writing by Phoenix Contact. Please note that the supplied documentation is product-specific documentation only and that you are responsible for checking the suitability and intended use of the products in your specific application, in particular with regard to observing the applicable standards and regulations. Although Phoenix Contact makes every effort to ensure that the information and content are accurate, up-to-date, and state-of-the-art, technical inaccuracies and/or printing errors in the information cannot be ruled out. Phoenix Contact does not offer any guarantees as to the reliability, accuracy, or completeness of the information. All information made available in the technical data is supplied without any accompanying guarantee, whether expressly mentioned, implied or tacitly assumed. This information does not include any guarantees regarding quality, does not describe any fair marketable quality, and does not make any claims as to quality guarantees or guarantees regarding the suitability for a special purpose.

Phoenix Contact accepts no liability or responsibility for errors or omissions in the content of the technical documentation (in particular data sheets, installation instructions, user manuals, etc.).

The aforementioned limitations of liability and exemptions from liability do not apply, in so far as liability must be assumed, e.g., according to product liability law, in cases of premeditation, gross negligence, on account of loss of life, physical injury or damage to health or on account of the violation of important contractual obligations. Claims for damages for the violation of important contractual obligations are, however, limited to contract-typical, predictable damages, provided there is no premeditation or gross negligence, or that liability is assumed on account of loss of life, physical injury, or damage to health. This ruling does not imply a change in the burden of proof to the detriment of the user.

Statement of legal authority

How to contact us

Internet

Up-to-date information on Phoenix Contact products and our Terms and Conditions can be found on the Internet at:
www.phoenixcontact.com

Make sure you always use the latest documentation.
It can be downloaded at:

www.phoenixcontact.net/catalog

Subsidiaries

If there are any problems that cannot be solved using the documentation, please contact your Phoenix Contact subsidiary.
Subsidiary contact information is available at www.phoenixcontact.com.

Published by

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
GERMANY
Phone +49 - (0) 52 35 - 3-00
Fax +49 - (0) 52 35 - 3-4 12 00

PHOENIX CONTACT
P.O. Box 4100
Harrisburg, PA 17111-0100
USA
Phone +1-717-944-1300

Should you have any suggestions or recommendations for improvement of the contents and layout of our manuals, please send your comments to:
tecdoc@phoenixcontact.com

Table of contents

1 Introduction 1-1

1.1 Device versions 1-3

2 Typical application scenarios 2-1

2.1 Stealth mode 2-1

2.2 Network router 2-2

2.3 DMZ 2-3

2.4 VPN gateway 2-3

2.5 WLAN via VPN 2-4

2.6 Resolving network conflicts 2-5

3 Operating elements and indicators 3-1

3.1 FL MGUARD RS 3-1

3.2 FL MGUARD GT/GT 3-2

3.2.1 Connecting the supply voltage and the VPN enable button 3-3

3.2.2 Using Smart mode 3-5

3.2.3 Messages in the 7-segment display 3-7

3.2.4 Interfaces on the FL MGUARD GT/GT 3-8

3.2.5 Signal contact 3-11

3.3 FL MGUARD SMARTSMART2/FL MGUARD SMART 3-14

3.4 FL MGUARD PCI 3-15

3.5 FL MGUARD BLADE 3-16

3.6 FL MGUARD DELTA 3-17

4 Startup 4-1

4.1 Safety notes 4-1

4.2 Checking the scope of supply 4-3

4.3 Installing the FL MGUARD RS 4-4

4.3.1 Mounting/removal 4-4

4.3.2 Connecting the supply voltage 4-5

4.3.3 Connecting to the network 4-6

4.4 Installing the FL MGUARD GT/GT 4-11

4.4.1 Mounting/removal 4-11

4.4.2 Connecting the supply voltage 4-12

4.4.3 Connecting to the network 4-14

4.5 Connecting the FL MGUARD SMART2/ FL MGUARD SMART 4-17

4.6 Installing the FL MGUARD BLADE 4-18

4.7 Connecting the FL MGUARD DELTA 4-20

4.8 Installing the FL MGUARD PCI 4-21

4.8.1 Driver mode 4-21

4.8.2 Power-over-PCI mode 4-23

4.8.3 Installing the hardware 4-24

4.8.4 Installing the driver 4-26

5 Preparing the configuration 5-1

5.1 Connection requirements 5-1
5.2 Local configuration on startup 5-3
5.2.1 Configuring the FL MGUARD on startup with stealth mode by default 5-4
5.2.2 Configuring the FL MGUARD on startup with router mode by default 5-9
5.2.3 Configuring the FL MGUARD on startup 5-10
5.3 Establishing a local configuration connection 5-13
5.4 Remote configuration 5-15

6 Configuration 6-1

6.1 Operation 6-1
6.2 Management menu 6-4
6.2.1 Management >> System Settings 6-4
6.2.2 Management >> Web Settings 6-20
6.2.3 Management >> Licensing 6-29
6.2.4 Management >> Update 6-32
6.2.5 Management >> Configuration Profiles 6-35
6.2.6 Management >> SNMP 6-38
6.2.7 Management >> Central Management 6-49
6.2.8 Management >> Restart 6-53
6.3 Blade Control menu 6-54
6.3.1 Blade Control >> Overview 6-54
6.3.2 Blade Control >> Blade 01 to 12 6-55
6.4 Network menu 6-57
6.4.1 Network >> Interfaces 6-57
6.4.2 Network >> NAT 6-97
6.4.3 Network >> DNS 6-102
6.4.4 Network >> DHCP 6-106
6.4.5 Network >> Proxy Settings 6-110
6.5 Authentication menu 6-111
6.5.1 Authentication >> Local Users 6-111
6.5.2 Authentication >> Firewall Users 6-113
6.5.3 Authentication >> Certificates 6-116
6.6 Network Security menu 6-130
6.6.1 Network Security >> Packet Filter 6-130
6.6.2 Network Security >> DoS Protection 6-142
6.6.3 Network Security >> User Firewall 6-144
6.7 CIFS Integrity Monitoring menu 6-147
6.7.1 CIFS Integrity Monitoring >> Importable Shares 6-148
6.7.2 CIFS Integrity Monitoring >> CIFS Integrity Checking 6-149

6.7.3 CIFS Integrity Monitoring >> CIFS Integrity Status 6-155
6.7.4 CIFS Integrity Monitoring >> CIFS AV Scan Connector 6-158
6.8 IPsec VPN menu 6-162
6.8.1 IPsec VPN >> Global 6-162
6.8.2 IPsec VPN >> Connections 6-170
6.8.3 Defining a new VPN connection/VPN connection channels 6-171
6.8.4 IPsec VPN >> L2TP over IPsec 6-194
6.8.5 IPsec VPN >> IPsec Status 6-195
6.9 SEC-Stick menu 6-196
6.9.1 Global 6-196
6.9.2 Connections 6-198
6.10 QoS menu 6-200
6.10.1 Ingress Filters 6-200
6.10.2 Egress Queues 6-203
6.10.3 Egress Queues (VPN) 6-204
6.10.4 Egress Rules 6-207
6.11 Redundancy menu 6-211
6.11.1 Ring/Network Coupling 6-211
6.12 Logging menu 6-212
6.12.1 Logging >> Settings 6-212
6.12.2 Logging >> Browse local logs 6-213
6.13 Support menu 6-217
6.13.1 Support >> Tools 6-217
6.13.2 Support >> Advanced 6-219
6.14 CIDR (Classless Inter-Domain Routing) 6-220
6.15 Network example diagram 6-221

7 Restart, recovery procedure, and flashing the firmware 7-1
7.1 Performing a restart 7-1
7.2 Performing a recovery procedure 7-2
7.3 Flashing the firmware/rescue procedure 7-3
7.3.1 Installing the DHCP and TFTP server 7-6

8 Glossary 8-1

9 Technical data 9-1
9.1 FL MGUARD RS 9-1
9.2 FL MGUARD GT/GT 9-2
9.3 FL MGUARD SMART2 9-4
9.4 FL MGUARD SMART 9-5
9.5 FL MGUARD PCI 9-6
9.6 FL MGUARD BLADE 9-7
9.7 FL MGUARD DELTA 9-8

9.8 Ordering data 9-9
9.8.1 Products 9-9
9.8.2 Accessories 9-9

1 Introduction

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

– Network card (FL MGUARD PCI) and switch (FL MGUARD DELTA).
– 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.

For additional information, please refer to the Innominate website: www.innominate.de.

Network features

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

Firewall features

– Stateful packet inspection
– Anti-spoofing
– IP filter
– L2 filter (only in stealth mode)
– NAT with FTP, IRC, and PPTP support (only in router modes)
– 1:1 NAT (only in *router* network mode)
– Port forwarding (not in *stealth* network mode)
– Individual firewall rules for different users (user firewall)
– Individual rule sets as action (target) of firewall rules (apart from user firewall or VPN firewall)
– Maximum firewall throughput up to 70 Mbps (160 Mbps FL MGUARD GT/GT)

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
- Recognition 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 (the "Firewall Redundancy" function is not available in firmware Version 7.0)
- Administration using SNMP v1 - v3 and Innominate Device Manager (IDM)
- PKI support for HTTPS/SSH remote access
- Can act as an NTP and DNS server via the LAN interface

Support

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

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

1.1 Device versions

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

FL MGUARD RS …

The **FL MGUARD RS** ... is available in five device versions:

– As a router - FL MGUARD RS-B
– As a router/firewall - FL MGUARD RS
– As a router/firewall with VPN - FL MGUARD RS VPN
– As a router/firewall with VPN and an integrated modem - FL MGUARD RS VPN ANALOG
– As a router/firewall with VPN and an integrated ISDN terminal adapter - FL MGUARD RS VPN ISDN

FL MGUARD GT/GT …

The **FL MGUARD GT/GT** ... is available in two device versions:

– As a security appliance - FL MGUARD GT/GT
– As a security appliance with VPN support - FL MGUARD GT/GT VPN

The device support hybrid use as a router/firewall/VPN router both via Ethernet and for serial dial-up line connections (not FL MGUARD GT/GT ...). The device is designed for DIN rail mounting (according to DIN EN 60715) and is therefore ideal for use in industrial applications.

VPN tunnels can be initiated using software or hardware switches. A redundant supply voltage can be connected (9 V DC ... 36 V DC).

Figure 1-1 FL MGUARD RS …

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 change existing system configurations or driver installations. 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**. To aid understanding, FL MGUARD SMART2 is mostly used for the two device versions in this user manual. The properties described also apply to the FL MGUARD SMART. Differences from the FL MGUARD SMART are indicated, if applicable.

Figure 1-2 FL MGUARD SMART2

FL MGUARD PCI

The **FL MGUARD PCI** is a card that can be used in a PCI slot. In *driver mode* it provides the computer in which the card is installed with all FL MGUARD functions, as well as acting as a normal network card.

In *power-over-PCI mode*, an existing network card in the computer or another computer/network can be connected.

Figure 1-3 FL MGUARD PCI

FL MGUARD BLADE

The **FL MGUARD BLADEPACK** comprises the FL MGUARD BLADEBASE, which can be installed easily in standard 3 U racks (19 inches), and up to 12 FL MGUARD BLADE devices, plus an FL MGUARD BLADE controller. This device version is therefore ideal for use in industrial applications, where several server systems can be protected individually and independently of one another.

An additional serial interface enables remote configuration via a telephone dial-up line connection or a terminal.

Figure 1-4 FL MGUARD BLADE

FL MGUARD DELTA

The **FL MGUARD DELTA** is a compact router with four port LAN switches (Ethernet/Fast Ethernet) and a pre-installed license for the operation of up to 250 VPN tunnels in parallel. This device is therefore ideal for use in logically segmented network environments, where the locally connected computers/networks share the FL MGUARD functions.

An additional serial interface enables configuration via a telephone dial-up line connection or a terminal. With its rugged metal housing, the FL MGUARD DELTA is suitable for installation in distribution compartments as well as for use as a desktop device.

Figure 1-5 FL MGUARD DELTA

2 Typical application scenarios

This section describes various application scenarios for the FL MGUARD.

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

2.1 Stealth mode

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

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

No configuration modifications are required on the computer itself.

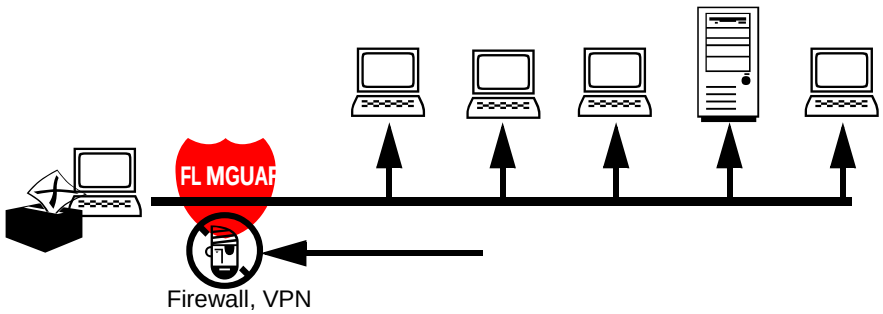


Figure 2-1 Stealth mode

2.2 Network router

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

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

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

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

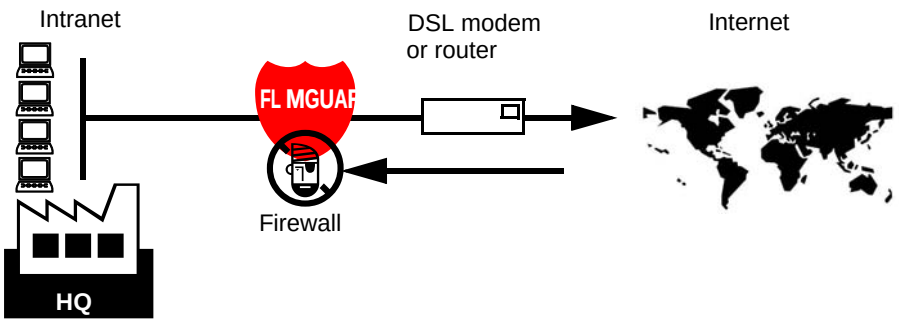


Figure 2-2 Network router

2.3 DMZ

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

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

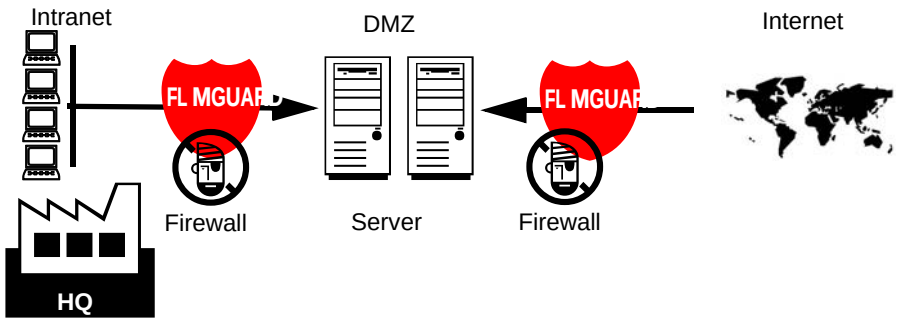


Figure 2-3 DMZ

2.4 VPN gateway

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

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

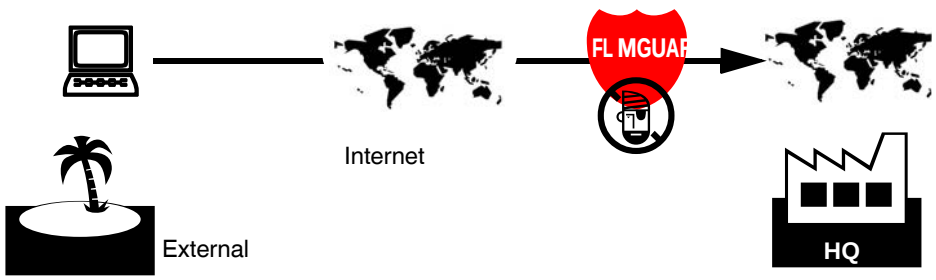


Figure 2-4 VPN gateway

2.5 WLAN via VPN

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

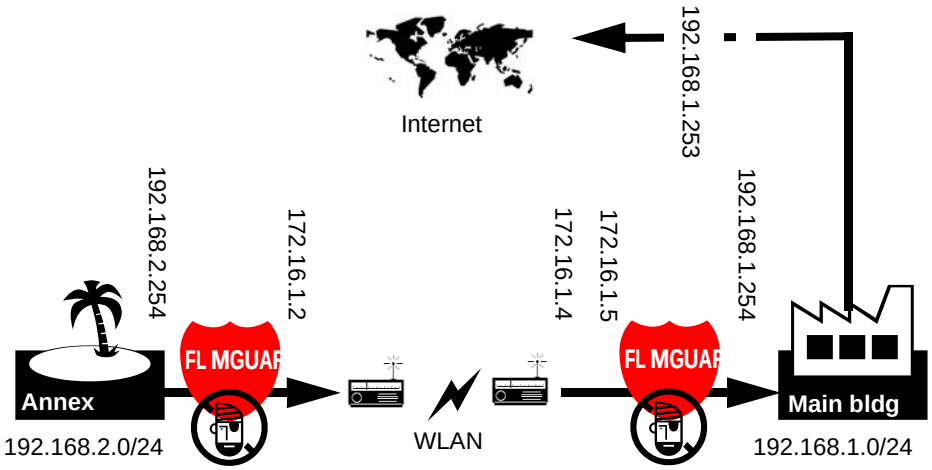


Figure 2-5 WLAN via VPN

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

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

Tunnel configuration in the annex

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

In the main building, the corresponding counterpart is configured:

Tunnel configuration in the main building

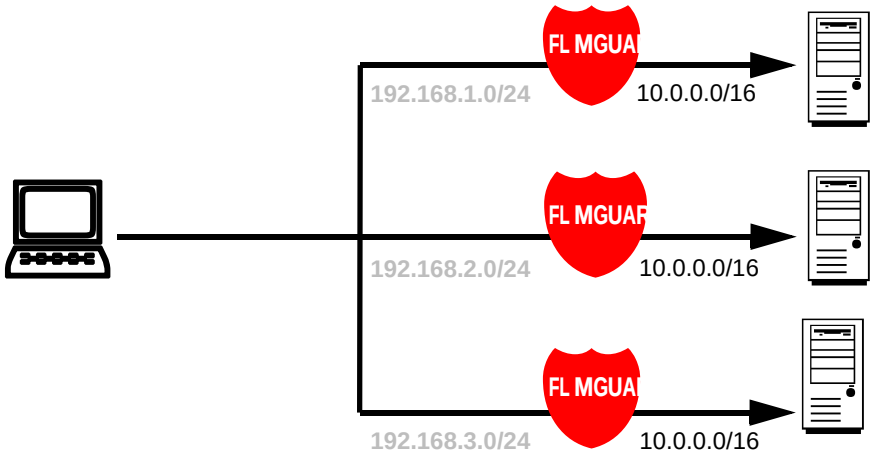
Connection type	Tunnel (network <-> network)
Local network	0.0.0.0
Address of the remote network	192.168.2.0/24

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

Default gateway in the main building

IP address of the default gateway	192.168.1.253

2.6 Resolving network conflicts



Resolving network conflicts

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

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

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

3 Operating elements and indicators

The FL MGUARD RS-B is a router, which offers static routing, NAT, 1:1 NAT, and port forwarding functions. Not all of the functions described in this user manual are supported by all device versions.

3.1 FL MGUARD RS ...

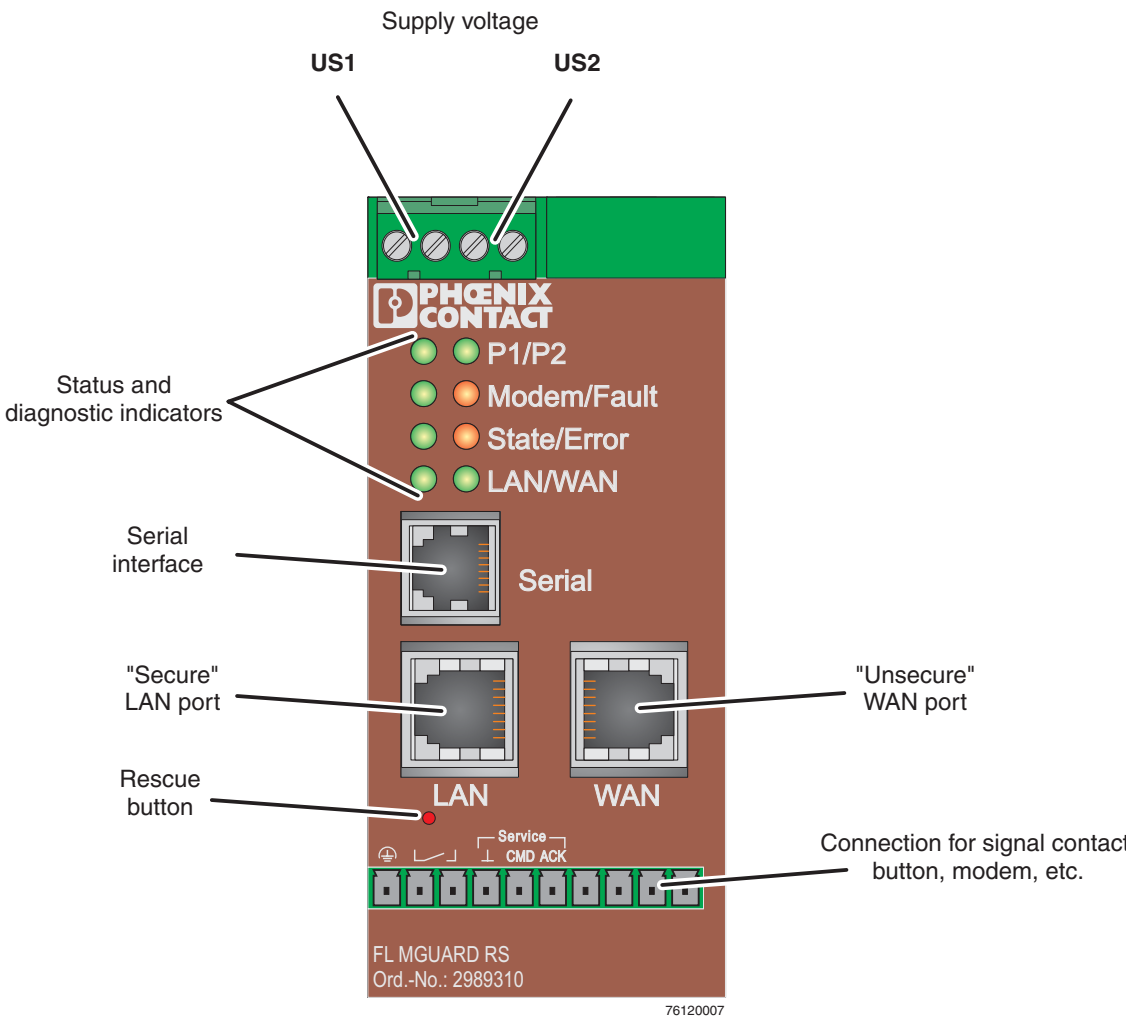


Figure 3-1 Operating elements and indicators on the FL MGUARD RS ...

Table 3-1 Indicators on the FL MGUARD RS ...

LED	State	Meaning
P1	Green ON	Power supply 1 is active
P2	Green ON	Power supply 2 is active
Modem	Green ON	Connection via modem established
Fault	Red ON	The signal contact is open due to an error. (The signal contact is interrupted during a restart.)
State	Flashing green	**Heartbeat**. The device is connected correctly and is operating.
Error	Flashing red	**System error**. Restart the device. – Press the Rescue button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the *recovery procedure* (see “Performing a recovery procedure” on page 7-2) or contact the Support team.
State + Error	Flashing alternately: green and red	**Boot process**. When the device has just been connected to the power supply. After a few seconds, this display changes to the heartbeat state.
LAN	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.
WAN	Green ON	

3.2 FL MGUARD GT/GT ...

By default upon delivery, the device is in router mode with the default IP address: 192.168.1.1, subnet mask: 255.255.255.0. The management interfaces can only be accessed via the LAN interface.

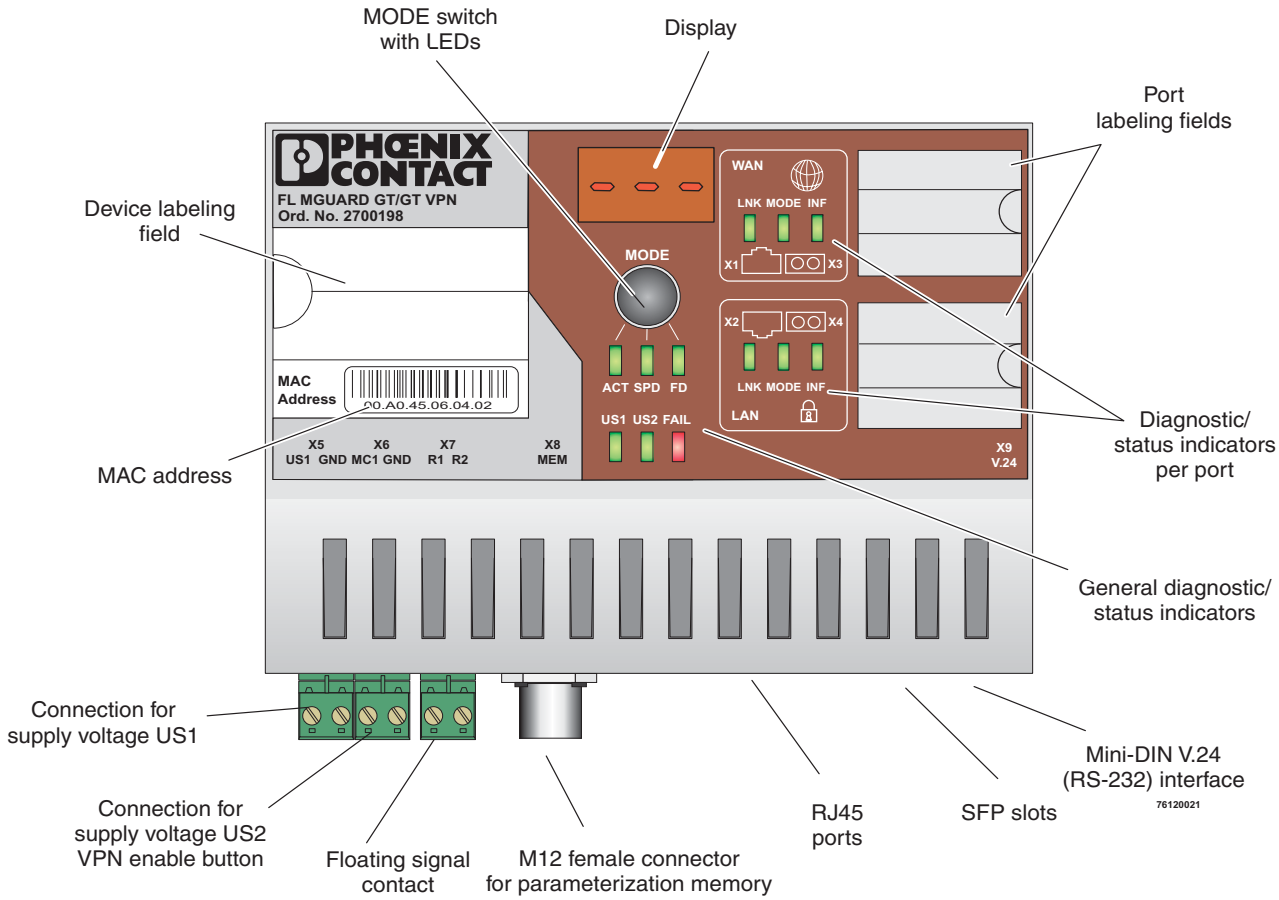


Figure 3-2 Operating elements and indicators on the FL MGUARD GT/GT ...

3.2.1 Connecting the supply voltage and the VPN enable button

The FL MGUARD GT/GT ... is operated using a 24 V DC voltage, which is applied via COMBICON terminal blocks X5 (US1 and GND).

COMBICON terminal blocks X6 (MC1 and GND) offer two functions:

- Connection of the redundant supply voltage with monitoring by the device
- Connection of a VPN enable button (for devices with VPN function)

3.2.1.1 Supplying the device using one voltage source

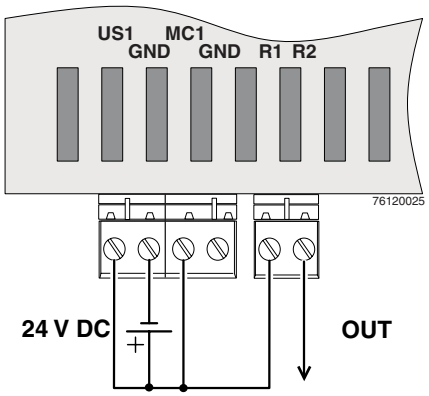


Figure 3-3 Supplying the device using one voltage source

3.2.1.2 Redundant 24 V DC supply

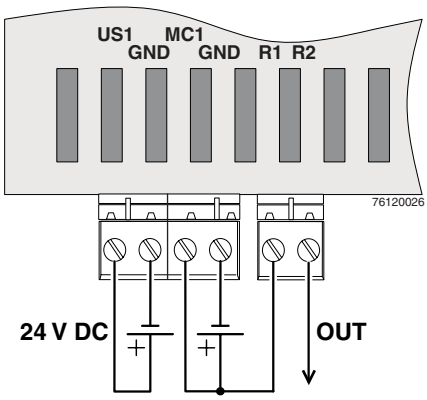


Figure 3-4 Supplying the device using two voltage sources

3.2.1.3 Supplying the device using one voltage source and connecting the VPN enable button

Always supply the VPN enable button from the voltage source that supplies the FL MGUARD GT/GT VPN.

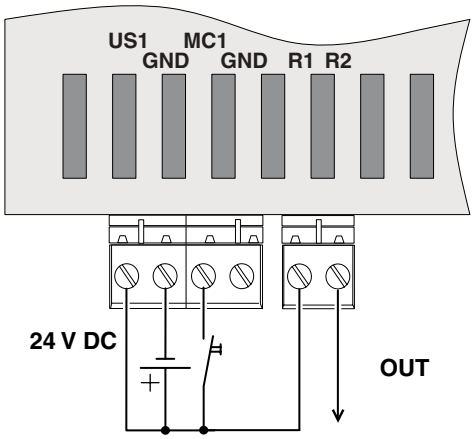


Figure 3-5 Supplying the device and connecting the VPN enable button using one voltage source

3.2.1.4 Redundant 24 V DC supply and connecting the VPN enable button

Always supply the VPN enable button from the voltage source that supplies the FL MGUARD GT/GT VPN.

NOTE: Risk of material damage. Only use power supplies that are suitable for parallel operation.

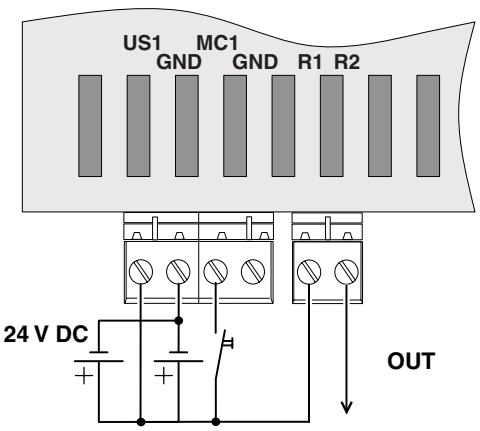


Figure 3-6 Supplying the device using two voltage sources

3.2.2 Using Smart mode

Smart mode enables the user to execute special functions without having to access the management interfaces.

The FL MGUARD GT/GT ... offers the following setting options in Smart mode:

– Execute the **recovery procedure**

– Apply a customized default profile
– Start the flash procedure
– Exit Smart mode without changes

3.2.2.1 Activating Smart mode

The mode button is used to call/exit Smart mode and to select the desired function. The three mode LEDs indicate the mode that is currently set and the mode that is entered when exiting Smart mode.

Calling Smart mode

- Disconnect the device from the power supply, if necessary.
- As soon as the supply voltage is switched on, hold down the mode button for **more than ten seconds**. These three mode LEDs flash briefly three times and indicate that Smart mode is active.
- When Smart mode is started, the device is initially in the "Exit without changes" state ("51" in the display).

Selecting the desired setting

- To select the different settings, press the mode button briefly and select the desired operating mode using a binary light pattern of the mode LEDs and a code on the 7-segment display.

Exiting Smart mode and activating the selection

- To exit, press and hold down the mode button for at least five seconds. The previously selected function is executed.

Possible functions in Smart mode

The device supports the selection of the following functions in Smart mode (see also example below):.

Table 3-2 Functions in Smart mode

Function	7-segment display	ACT LED 1	SPD LED 2	FD LED 3
Exit Smart mode without changes	51	OFF	OFF	**ON**
Activate the recovery procedure	55	**ON**	OFF	**ON**
Activate the flash procedure	56	**ON**	**ON**	OFF
Apply customized default profile	57	**ON**	**ON**	**ON**

3.2.3 Messages in the 7-segment display

During error-free operation:

Indication	Meaning
bo	Extracting/starting firmware (boot)
01	The device is in normal operating mode and tries to obtain network parameters from a BootP/DHCP server using DHCP requests
03	Downloading firmware via TFTP
04	Loading firmware in the Flash memory that was loaded via the network
05	The recently loaded firmware was successfully saved in the Flash memory
06	New firmware was successfully saved in the Flash memory, a rollout script was downloaded via TFTP and executed
08	The device is in rescue mode and tries to obtain network parameters from a BootP/DHCP server using DHCP requests in order to request a firmware image
_ _ _	Initializing firmware
- - -	Firmware running in normal mode
rB	Device rebooting
R0	Recovery procedure is deactivated according to the installed customized default profile
0d	Customized default profile cannot be applied (e.g., it is not installed)

Messages during operation with the memory module:

Indication	Meaning
5c	Save configuration data on the MEM PLUG
EC	Equal configuration - the configurations on the MEM PLUG and the device are the same
dC	Different configuration - the configurations on the MEM PLUG and the device are different
0C	The MEM PLUG is empty
FC	Not enough memory on the memory module to save the configuration
HC	This MEM PLUG is not compatible with the device, e.g., a wireless ID plug or an MRP master

Messages in Smart mode:

Indication	Meaning
51	Smart mode "No changes"
55	Smart mode "Recovery procedure"
56	Smart mode "Flash procedure"
57	Smart mode "Customized default profile"

In the event of an error:

Indication	Meaning	Remedy
41	RAM test error	– Perform a voltage reset
42	Flash test error	– Perform a voltage reset
07	Error when executing the rollout script	– Check the rollout script for errors
17	Firmware transfer via TFTP or Xmodem failed (display changes from "03" to "17")	– Check the physical connection. – Establish a point-to-point connection. – Make sure that the file (with the specified file name) exists and is in the correct directory. – Check the IP address of the TFTP server. – Activate the TFTP server. – Repeat the download.
19	File transfer was completed successfully, but the file is not a valid firmware version for the device	– Provide a valid firmware version with the previously specified file name. – Repeat the download.
30	Device temperature too high or too low	– The device has exited the temperature range set in the web interface.
49	SFP module not supported or faulty	– Replace the SFP module with a supported and/or fully functional SFP module
HC	This MEM PLUG is not compatible with the device, e.g., a wireless ID plug or an MRP master	– Use a suitable MEM PLUG.

The points under "Remedy" are recommendations; they do not all have to be carried out for every error.

For all other message codes that are not listed here, please contact Phoenix Contact.

3.2.4 Interfaces on the FL MGUARD GT/GT ...

3.2.4.1 RJ45 ports

The FL MGUARD GT/GT ... has two RJ45 ports, which support both 10/100 Mbps and 1000 Mbps and can be configured via web-based management.

The LAN or WAN RJ45 ports are disabled after the next reboot of the device if an SFP module is inserted in the corresponding slot.

Assignment of the RJ45 Ethernet connectors

Please note that for operation with 1000 Mbps (Gigabit), cables with four twisted pairs (eight wires), which meet the requirements of Cat 5e as a minimum, must be used.

Table 3-3 Pin assignment of RJ45 connectors

Pin	10Base-T/10 Mbps	100Base-T/100 Mbps	100Base-T/1000 Mbps
1	TD+ (transmit)	TD+ (transmit)	BI_DA+ (bidirectional)
2	TD- (transmit)	TD- (transmit)	BI_DA- (bidirectional)
3	RD+ (receive)	RD+ (receive)	BI_DB+ (bidirectional)
4	-	-	BI_DC+ (bidirectional)
5	-	-	BI_DC- (bidirectional)
6	RD- (receive)	RD- (receive)	BI_DB- (bidirectional)
7	-	-	BI_DD+ (bidirectional)
8	-	-	BI_DD- (bidirectional)

3.2.4.2 SFP slots

Inserted SFP modules are detected automatically when the device is switched on and the corresponding RJ45 port is disabled. Configuration of the SFP modules is not required because the modules are always operated at 1000 Mbps full duplex.

Use of the following module types is recommended:

– FL SFP SX, Order No. 2891754
– FL SFP LX, Order No. 2891767
– FL SFP LH, Order No. 2989912

Use of SFP slots

The SFP slots are used by SFP modules (fiber optic fiberglass modules in SFP format). By selecting SFP modules, the user can specify whether the switch has multi-mode or single-mode fiber optic ports, for example.

The SFP modules are available separately as accessories, see “Products” on page 9-9.

Elements of the SFP modules

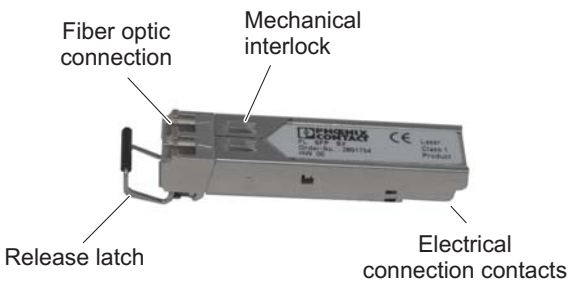


Figure 3-7 Elements of the SFP modules

3.2.4.3 Mounting the SFP modules

Inserting the SFP modules

- Insert the SFP modules in the relevant slots on the switch.

- Ensure correct mechanical alignment of the SFP modules.

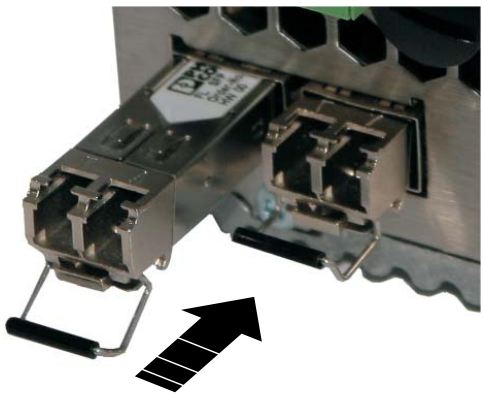


Figure 3-8 Inserting the SFP modules

Connecting the fiber optic cable

- Ensure correct mechanical alignment when inserting the fiber optic connectors.

Removing the fiber optic connectors

- Press the arresting latch (A) and pull out the connector (B).

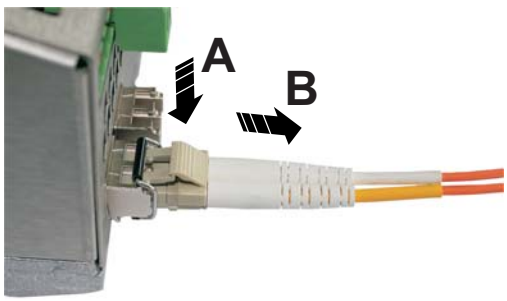


Figure 3-9 Removing the fiber optic connectors

Removing the SFP modules

- Remove the fiber optic connector before removing the SFP module.

- Flip down the release latch (A) and pull out the SFP module (B).

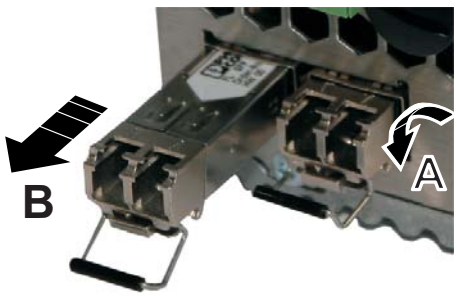


Figure 3-10 Removing the SFP modules

RS-232 interface for external management

The interface is designed **exclusively for configuration purposes** and not for the connection of external devices such as modems.

The 6-pos. Mini-DIN female connector provides a serial interface to connect a local management station. It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface. Set the following transmission parameters:

Bits per second	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

RS-232 (V.24) interface

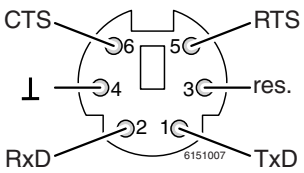


Figure 3-11 Transmission parameters and assignment of the RS-232 interface

3.2.5 Signal contact

The switch has a floating signal contact. An error is indicated when the contact is opened.

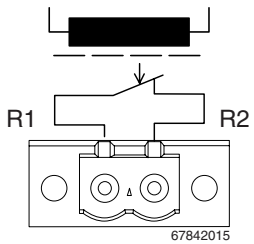


Figure 3-12 Basic circuit diagram for the signal contact

3.2.5.1 Local diagnostic and status indicators on the FL MGUARD GT/GT ...

Table 3-4 Indicators on the FL MGUARD GT/GT ...

Des.	Color	Status	Meaning
US1	Green	ON	Supply voltage 1 in the tolerance range
		OFF	Supply voltage 1 too low
US2	Green	ON	Supply voltage 2 in the tolerance range
		OFF	Supply voltage 2 too low
FAIL	Red	ON	Signal contact open, i.e., an error has occurred
		OFF	Signal contact closed, i.e., an error has not occurred
A Link LED is located on the front of the device for the LAN and WAN port.			
LNK (Link)	Green	ON	Link active
		OFF	Link not active
Another LED is located on the front of the device for the LAN and WAN port. The function of the second LED (MODE) for each port can be set using the MODE switch (see also example below). There are three options (during the boot process the mode and port LEDs are permanently on):			
ACT (Activity)	Green	ON	Receiving telegrams
		OFF	Not receiving telegrams
SPD (Speed)	Green/ orange	ON (orange)	1000 Mbps
		ON (green)	100 Mbps (for RJ45 ports only)
		OFF	10 Mbps if link LED is active (for RJ45 ports only)
FD (Duplex)	Green	ON	Full duplex
		OFF	Half duplex
ACT/SPD/FD	Yellow	Flashing	The device is in Smart mode (see “Using Smart mode” on page 3-5)
INF (Duplex)	Green	ON	VPN tunnel established
		Flashing	Initializing VPN tunnel
		OFF	No VPN tunnel

Example:

In Figure 3-13, the LED indicators have the following meaning:

A: The MODE switch has been set to display the duplex mode (FD); the mode LEDs now indicate that the LAN port is in half duplex mode and the WAN port is in full duplex mode.

B: The switch has been set to display the Activity (ACT); the mode LEDs now indicate that incoming data packets are detected on both ports.

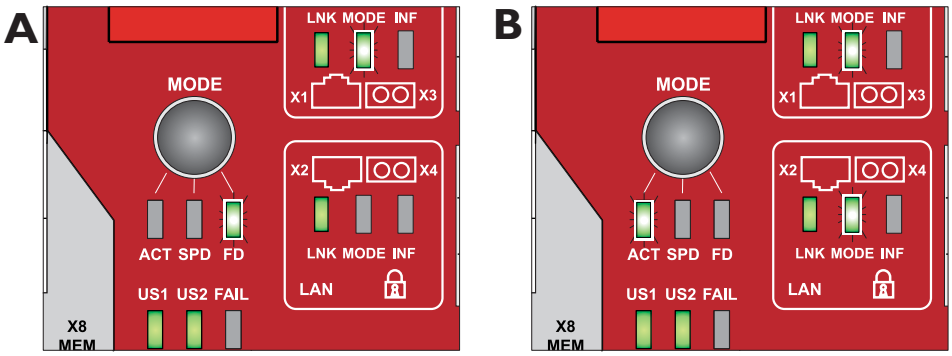


Figure 3-13 Example for status indicators on the FL MGUARD GT/GT ...

3.3 FL MGUARD SMARTSMART2/FL MGUARD SMART

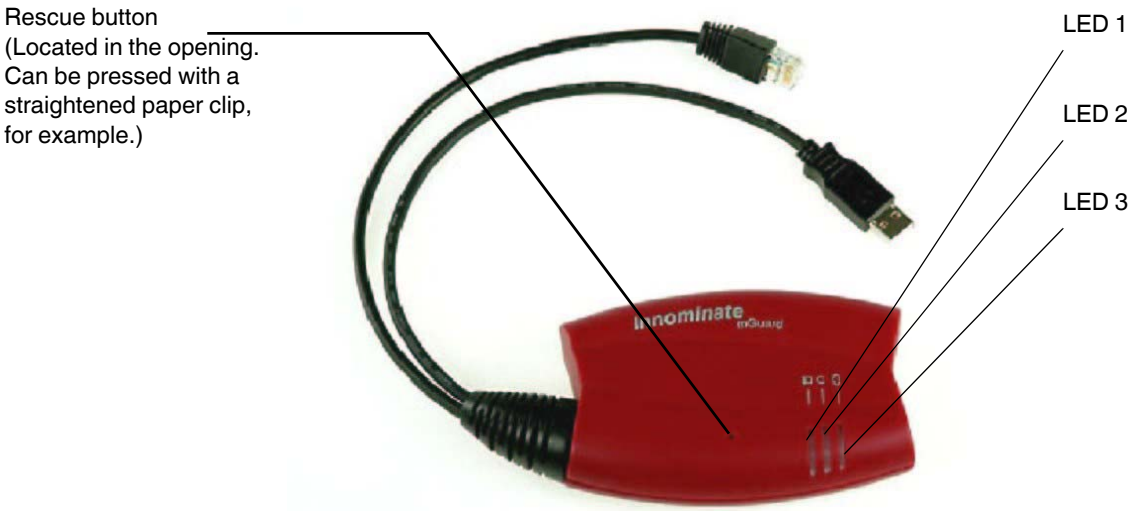


Figure 3-14 Operating elements and indicators on the FL MGUARD SMART2

Table 3-5 Indicators on the FL MGUARD SMART2

LEDs	Color	State	Meaning
2	Red/green	Flashing red/green	**Boot process**. When the device has just been connected to the power supply. After a few seconds, this display changes to the heartbeat state.
	Green	Flashing	**Heartbeat**. The device is connected correctly and is operating.
	Red	Flashing	**System error**. Restart the device. • Press the Rescue button (for 1.5 seconds). • Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the *recovery procedure* (see “Performing a recovery procedure” on page 7-2) or contact the Support team.
1 and 3	Green	ON or flashing	**Ethernet status**. LED 1 indicates the status of the LAN port, LED 3 the status of the WAN port. As soon as the device is connected to the network, a continuous light indicates that there is a connection to the network partner. When data packets are transmitted, the LED goes out briefly.
1, 2, 3	Various LED light codes		**Recovery mode**. After pressing the **Rescue** button. See “Restart, recovery procedure, and flashing the firmware” on page 7-1.

3.4 FL MGUARD PCI

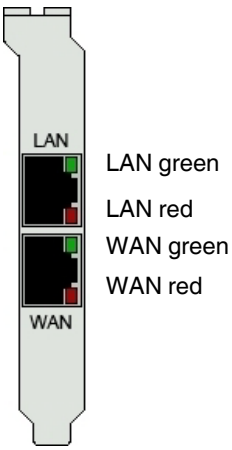


Figure 3-15 Operating elements and indicators on the FL MGUARD PCI ...

Table 3-6 Indicators on the FL MGUARD PCI ...

LEDs	Color	State	Meaning
WAN, LAN	**Red**	Flashing	**Boot process**. When the computer is started or restarted.
WAN	**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 7-2) or contact the Support team.
WAN, LAN	**Green**	ON or flashing	**Ethernet status**. Indicates the status of the LAN or WAN interface. As soon as the device is connected, a continuous light indicates that there is a connection to the network partner. When data packets are transmitted, the LED goes out briefly.
WAN **LAN**	**Red green** **Green**	Various LED light codes	**Recovery mode**. After pressing the **Rescue** button*****. See “Restart, recovery procedure, and flashing the firmware” on page 7-1

***** On the FL MGUARD PCI ..., the Rescue button is on the PCB (see “Installing the hardware” on page 4-24).

3.5 FL MGUARD BLADE

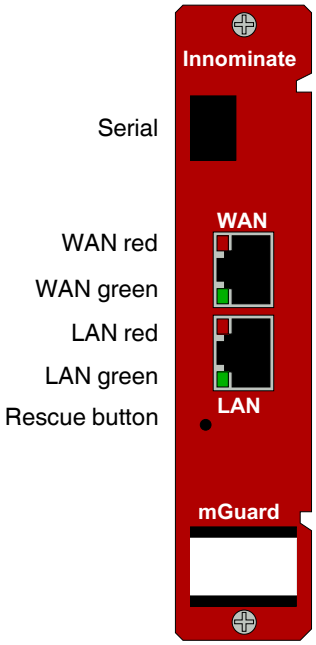


Figure 3-16 Operating elements and indicators on the FL MGUARD BLADE ...

Table 3-7 FL MGUARD BLADE

LEDs	Color	State	Meaning
WAN, LAN	**Red**	Flashing	**Boot process**. When the computer is started or restarted.
WAN	**Red**	Flashing	**System error**. Restart the device. • Press the Rescue button (for 1.5 seconds). If the error is still present, start the *recovery procedure* (see “Performing a recovery procedure” on page 7-2) or contact the Support team.
WAN, LAN	**Green**	ON or flashing	**Ethernet status**. Indicates the status of the LAN or WAN interface. As soon as the device is connected, a continuous light indicates that there is a connection to the network partner. When data packets are transmitted, the LED goes out briefly.
WAN **LAN**	**Green** **Red** **Green**	Various LED light codes	**Recovery mode**. After pressing the **Rescue** button. See “Restart, recovery procedure, and flashing the firmware” on page 7-1

3.6 FL MGUARD DELTA

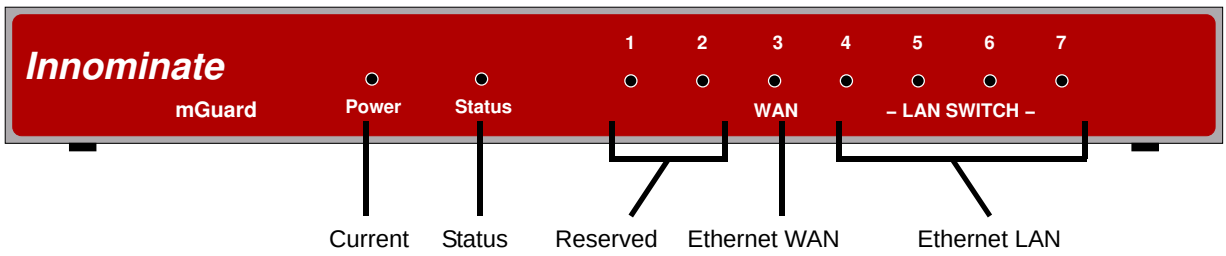


Figure 3-17 Operating elements and indicators on the FL MGUARD DELTA

Table 3-8 Indicators on the FL MGUARDDELTA

LEDs	State	Meaning
Power	ON	**The power supply is active.**
Status	ON	The FL MGUARD is starting.
	Heartbeat (Flash, flash, pause, etc.)	The FL MGUARD is ready.
1.2	–	**Reserved**
3 (WAN)	ON	**Link present**
	Flashing	Data transfer
4 - 7 (LAN)	ON	Link present
	Flashing	Data transfer

4 Startup

4.1 Safety notes

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

WARNING: Intended use

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

WARNING: Only connect LAN installations to RJ45 female connectors

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

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

General notes regarding usage

NOTE: Connection notes

- A free PCI slot (3.3 V or 5 V) must be available on your PC when using the FL MGUARD PCI.
- Do not bend connecting cables. Only use the network connector for connection to a network.

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C to +40°C (FL MGUARD SMART2, FL MGUARD BLADE, FL MGUARD DELTA),
  70°C, maximum (FL MGUARD PCI),
  55°C, maximum (FL MGUARD RS ...)
  -20°C to 60°C (FL MGUARD GT/GT, FL MGUARD GT/GT VPN)
- Maximum humidity 90%, no condensation
  (FL MGUARD SMART, FL MGUARD BLADE, FL MGUARD DELTA, FL MGUARD PCI)
  Maximum humidity 95%, no condensation
  (FL MGUARD RS..., FL MGUARD GT/GT, FL MGUARD GT/GT VPN)

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

NOTE: Cleaning

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

Steps for startup

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

Table 4-1 Steps for startup

Step	Aim	Page
1	Check the scope of supply Read the release notes	“Checking the scope of supply” on page 4-3
2	Connect the device	“Installing the FL MGUARD RS ...” on page 4-4 “Installing the FL MGUARD GT/GT ...” on page 4-11 “Connecting the FL MGUARD SMART2/ FL MGUARD SMART” on page 4-17 “Installing the FL MGUARD BLADE” on page 4-18 “Connecting the FL MGUARD DELTA” on page 4-20 “Installing the FL MGUARD PCI” on page 4-21
3	Configure the device, if required. Work through the individual menu options offered by the FL MGUARD configuration interface. Read the explanations in this user manual in order to determine which settings are required for your operating environment.	“Local configuration on startup” on page 5-3

4.2 Checking the scope of supply

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

The scope of supply includes:

– FL MGUARD RS … , FL MGUARD BLADE, FL MGUARD DELTA, FL MGUARD PCI or FL MGUARD SMART2.
– Package slip

The FL MGUARD RS ... also includes:

– Terminal block for the power supply connection (inserted)
– Terminal block for the signal contact, button, and optional ISDN or telephone connection

The FL MGUARD GT/GT ... also includes:

– Terminal block for the power supply connection (inserted)
– Terminal block for the signal contact, button

The FL MGUARD BLADEPACK also includes:

– 19" FL MGUARD BLADEBASE
– One FL MGUARD BLADE as the controller
– Two power supply units
– Two power cables
– 12 place holders
– 12 labeling plates M1 to M12
– Screws for mounting the FL MGUARD BLADEBASE

The FL MGUARD DELTA also includes:

– One 5 V DC power supply unit
– Two UTP Ethernet cables

4.3 Installing the FL MGUARD RS ...

WARNING:
The housing must not be opened.

WARNING:
The shielding ground of the connected twisted pair cables is electrically connected to the front plate.

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. When installed in residential or office areas, the Innominate FL MGUARD RS ... may only be operated in control cabinets with fire protection properties according to EN 60950-1.

4.3.1 Mounting/removal

Mounting

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

- Pull out the terminal block from the bottom of the FL MGUARD RS ... and wire the signal lines and other connections as required (see “Connection options on lower terminal strip” on page 4-7).
- Tighten the screws on the screw terminal blocks with at least 0.22 Nm.
  Wait to insert the terminal block.
- Mount the FL MGUARD RS ... on a grounded 35 mm DIN rail according to DIN EN 60715.
  The device conducts the grounding provided by the DIN rail through the left-hand contact (ground connection) of the lower terminal strip.

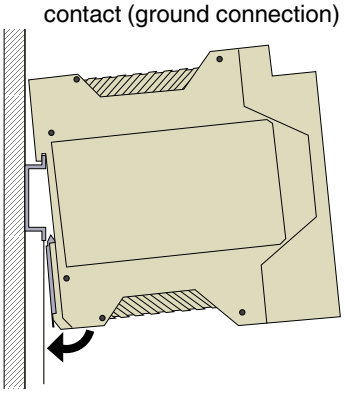


Figure 4-1 Mounting the FL MGUARD RS ... on a DIN rail

- Attach the top snap-on foot of the FL MGUARD RS ... to the DIN rail and then press the FL MGUARD RS ... down towards the DIN rail so that it engages with a click.
- Insert the wired terminal block.
- Connect the supply voltage at the top of the terminal block (see “Connecting the supply voltage” on page 4-5).
- Make any necessary network connections at the LAN port or WAN port (see “Connecting to the network” on page 4-6).

- Connect the corresponding device at the Serial port as required (see “Serial port” on page 4-10).

Removal

- Remove or disconnect the connections.
- To remove the FL MGUARD RS ... 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 RS ...

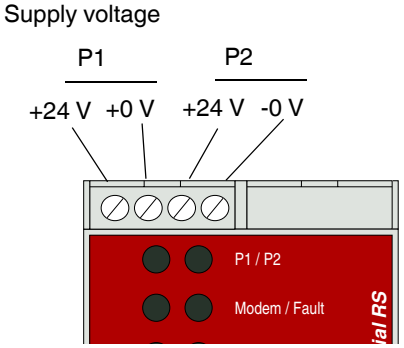
4.3.2 Connecting the supply voltage

WARNING:

The FL MGUARD RS ... is designed for operation with a DC voltage of 9 V DC ... 36 V DC/SELV, 0.5 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 terminal block with screw locking, which is located on the top of the device.



Supply voltage

– NEC Class 2 power source 12 V DC or 24 V DC
– -25% +33% SELV (SELV/PELV, redundant inputs isolated)
– 5 A, maximum
– Buffer time 10 ms, minimum at 24 V DC

Redundant power supply

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

If the supply voltage is not redundant, the FL MGUARD RS ... indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs.

4.3.3 Connecting to the network

WARNING:

Only connect the FL MGUARD network ports to LAN installations.

When connecting to the network, use cables with bend protection on the connectors.

Cover unused female connectors with the dust protection caps provided.

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

LAN port

- Connect the local computer or the local network to the LAN port of the FL MGUARD using a UTP Ethernet cable (CAT5). If your computer is already connected to a network, patch the FL MGUARD between the existing network connection.

Please note that configuration can only be completed via the LAN interface and that the firewall of the FL MGUARD RS prevents all IP data traffic from the WAN to the LAN interface.

WAN port

- Use a UTP cable (CAT5).
- Connect the external network via the WAN female connector, e.g., WAN, Internet. (Connections to the remote device or network are established via this network.)

Driver installation is not required.

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

Connection options on lower terminal strip

The FL MGUARD RS ... is available in three versions, which can be distinguished by the connection options on the lower terminal strip:

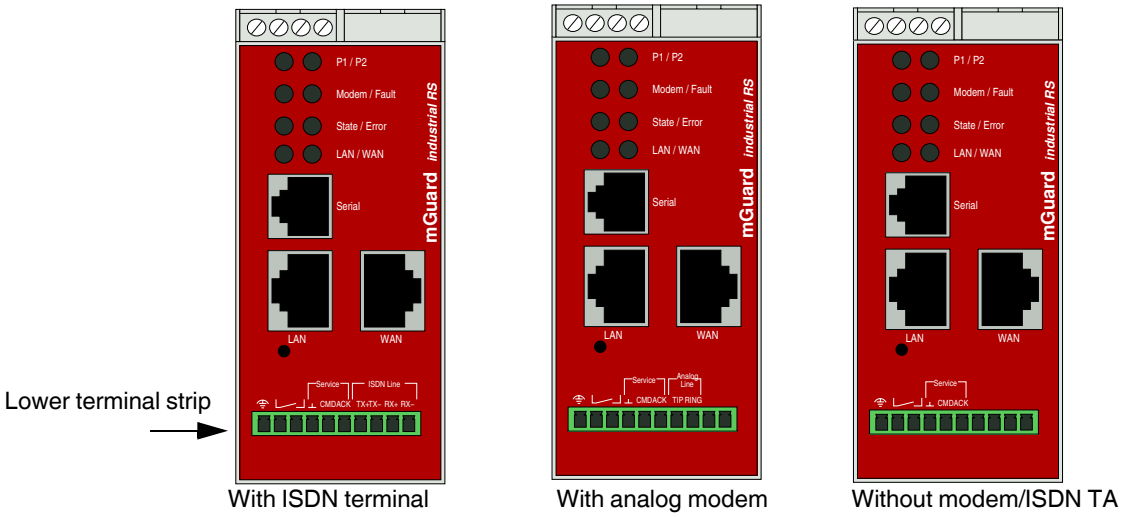


Figure 4-2 FL MGUARD RS ...: Lower terminal strip

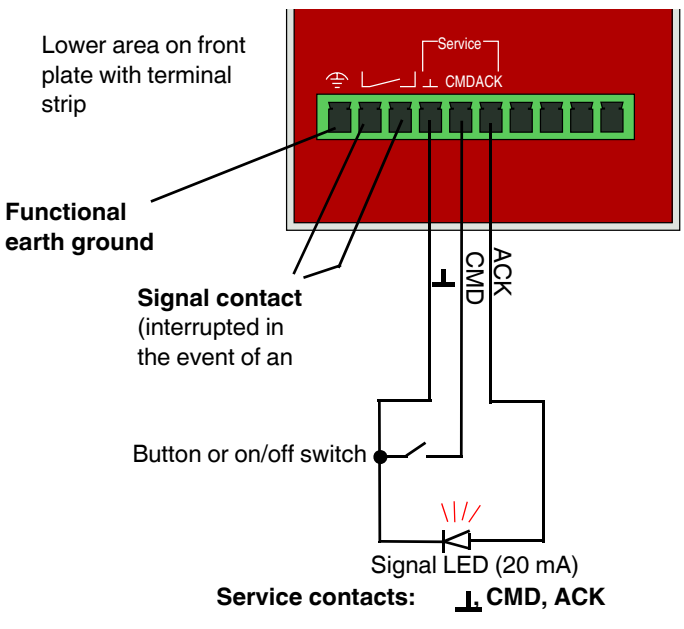


Figure 4-3 FL MGUARD RS ... : Without modem/ISDN terminal adapter

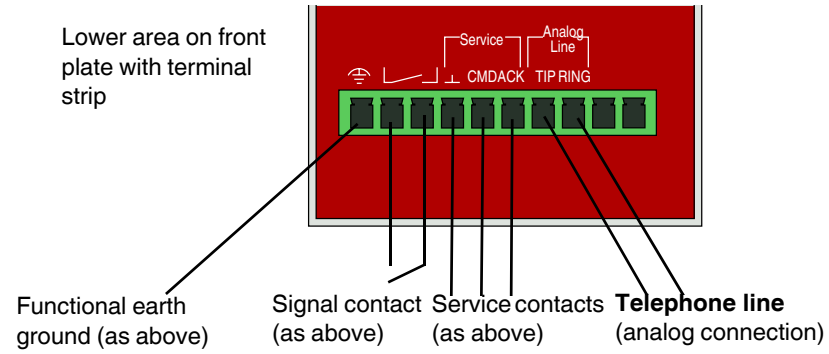


Figure 4-4 FL MGUARD RS ... **with modem**

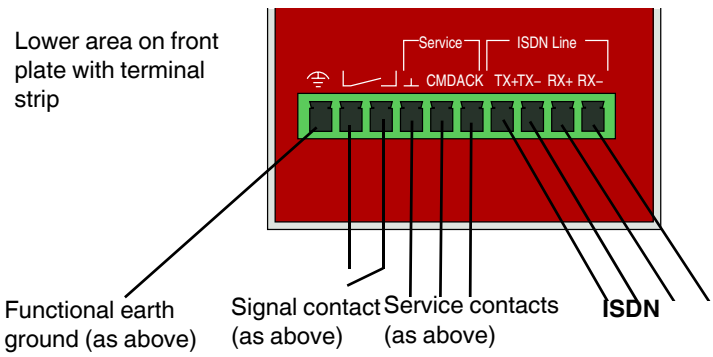


Figure 4-5 FL MGUARD RS ... **with ISDN terminal adapter**

Functional earth ground

The functional earth ground can be used by the operator. This connection is electrically connected to the back of the FL MGUARD RS .... The FLMGUARD RS ... is grounded when it is mounted on a DIN rail with the metal clamp, which connects the back of the device to the DIN rail. The DIN rail must be grounded.

Signal contact

WARNING: Only SELV circuits with voltage limitations according to EN 60950-1 may be connected to the signal contact.

The signal contact monitors the operation of the FL MGUARD RS ... and thus enables remote diagnostics. Interruption of the contact via the floating signal contact (relay contact, closed current circuit) indicates the following:

– Failure of at least one of the two supply voltages.
– Power supply of the FLMGUARD RS ... below the specified limit value (supply voltage 1 and/or 2 is less than 9 V).
– The faulty link status of at least one port. The link status message for each port can be masked on the FL MGUARD RS ... via the management software.
  By default upon delivery, there is no connection monitoring.
– Error during selftest.

During a restart, the signal contact is interrupted until the FL MGUARD has started up completely. This also applies when the signal contact is manually set to *Closed* in the software configuration.

Service contacts

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

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

A standard **LED** (up to 3.5 V) or a corresponding optocoupler can be connected between **contacts ACK (+) and** _I_ **(-)**. The contact is short-circuit-proof and supplies 20 mA, maximum. The LED or optocoupler must be connected without preresistor (for wiring, see Figure 4-3 to Figure 4-5).

The **button** or **on/off switch** is used to establish and release a predefined VPN connection. The LED indicates the status of the VPN connection (see “IPsec VPN >> Global” on page 6-162 under "Options").

Operating a connected button

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

Operating a connected on/off switch

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

Signal LED

If the signal LED 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 signal LED is ON, the VPN connection is present.

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

Analog line (for integrated modem)

WARNING: The analog connections (TIP, RING) should only be connected to the telecommunications cable provided.

The TIP and RING contacts are for connection to the fixed-line telephone network (analog connection).

For the contact designations specified on the front plate, the following designations are usually used in Germany:

TIP = a **RING = b**

ISDN line (with integrated ISDN terminal adapter)

WARNING: The ISDN connections (TX+, TX-, RX+, RX-) should only be connected to an ISDN S0 bus.

Contacts TX+, TX-, RX+, and RX- are designed for connection to ISDN and identify the FL MGUARD RS ISDN as a device in the ISDN network. The table below describes the assignment of the contacts to 8-pos. connections both for connectors and for sockets, for example RJ45:

Table 4-2 Assignment of the contacts to 8-pos. connections

Pos. number	TE (FL MGUARD)
3	TX+
4	RX+
5	RX-
6	TX-

Serial port

WARNING: The serial interface (RJ12 female connector) must not be connected directly to the telecommunications connections. To connect a serial terminal or a modem, use a serial cable with RJ12 connector. The maximum cable length of the serial cable is 30 m.

The serial port (serial interface) can be used as follows:

To configure the FL MGUARD via the serial interface. There are two options:

– A PC is connected directly to the serial interface of the FL MGUARD (via the serial interface of the PC). The PC user can then use a terminal program to configure the FL MGUARD via the command line.

– 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 user of a remote PC, which is also connected to the telephone network by a modem, can then establish a PPP (Point-to Point Protocol) dial-up line connection to the FL MGUARD and configure it via a web browser.

To manage data traffic via the serial interface instead of via the WAN interface of the FL MGUARD. In this case, a modem should be connected to the serial interface.

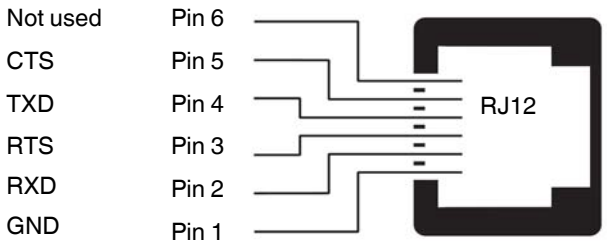


Figure 4-6 Pin assignment of the RJ12 female connector (serial port)

On the FL MGUARD RS ... with integrated modem or ISDN terminal adapter, data traffic can be transmitted via the *analog line* or *ISDN line* connections instead of via the WAN interface.

4.4 Installing the FL MGUARD GT/GT ...

WARNING:
The housing must not be opened.

WARNING:
The shielding ground of the connected twisted pair cables is electrically connected to the front plate.

4.4.1 Mounting/removal

Mounting

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

- Pull out the terminal block from the bottom of the FL MGUARD GT/GT ... and wire the connections as required (see “Connection options on lower terminal strip” on page 4-7).
- Tighten the screws on the screw terminal blocks with at least 0.22 Nm.
  Wait to insert the terminal block.
- Mount the FL MGUARD GT/GT... on a grounded 35 mm DIN rail according to DIN EN 60715.
  The device is grounded by snapping it onto a grounded DIN rail.

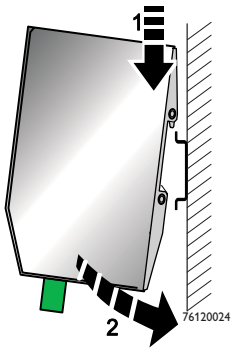


Figure 4-7 Mounting the FL MGUARD GT/GT ... on a DIN rail

- Attach the top snap-on foot of the FL MGUARD GT/GT ... to the DIN rail and then press the FL MGUARD GT/GT ... down towards the DIN rail so that it engages with a click.
- Insert the required wired terminal blocks.
- Make any necessary network connections at the LAN port or WAN port (see “Connecting to the network” on page 4-6).
- Connect the corresponding device at the serial port as required (see “Serial port” on page 4-10).

Removal

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

4.4.2 Connecting the supply voltage

Please note that there are several options when connecting the supply voltage and the optional VPN enable button/signal contact:

- **Simple** connection of the supply voltage/signal contact **without** VPN enable button
- **Simple** connection of the supply voltage/signal contact **with** VPN enable button
- **Redundant** connection of the supply voltage/signal contact **without** VPN enable button
- **Redundant** connection of the supply voltage/signal contact **with** VPN enable button

The MC1/GND connection terminal blocks can be used either for the connection of a (redundant) power supply or a VPN enable button.

WARNING:

The FL MGUARD GT/GT ... is designed for operation with a DC voltage of 18 V DC ... 32 V DC/SELV, 0.5 A maximum.

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

4.4.2.1 Simple connection of the supply voltage/signal contact without VPN enable button

The supply voltage is connected via a terminal block with screw locking, which is located under the front of the device.

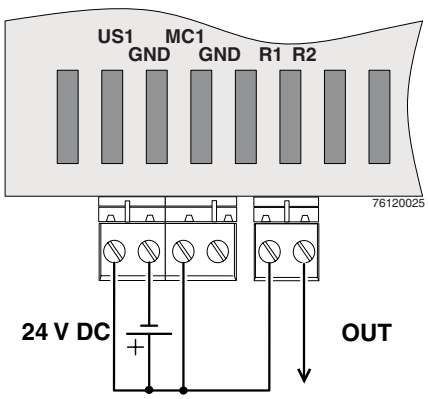


Figure 4-8 Simple connection of the supply voltage/signal contact without VPN enable button

4.4.2.2 Redundant connection of the supply voltage/signal contact without VPN enable button

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

If the supply voltage is not redundant, the FLMGUARD GT/GT... indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs.

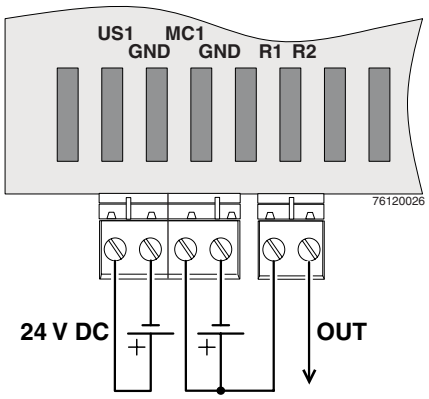


Figure 4-9 Redundant connection of the supply voltage/signal contact without VPN enable button

4.4.2.3 Simple connection of the supply voltage/signal contact with VPN enable button

Always supply the VPN enable button from the voltage source that supplies the FL MGUARD GT/GT VPN.

To enable a VPN enable button/switch connected externally to the device to establish/release a VPN tunnel, this switch/button should be connected to MC1/GND.

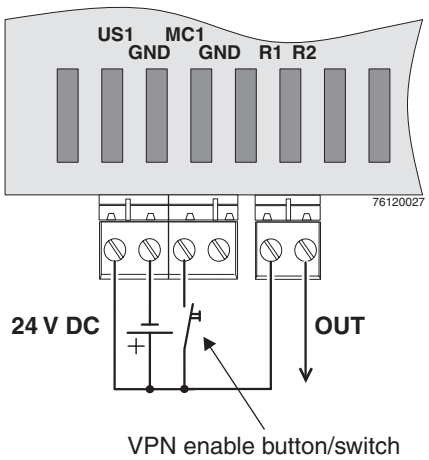


Figure 4-10 Simple connection of the supply voltage/signal contact with VPN enable button

4.4.2.4 Redundant connection of the supply voltage/signal contact with VPN enable button

NOTE: Risk of material damage - Only use power supplies that are suitable for parallel operation.

Always supply the VPN enable contact from the voltage source that supplies the FL MGUARD GT/GT VPN.

To enable a VPN enable button/switch connected externally to the device to establish/release a VPN tunnel, this switch/button should be connected to MC1/GND.

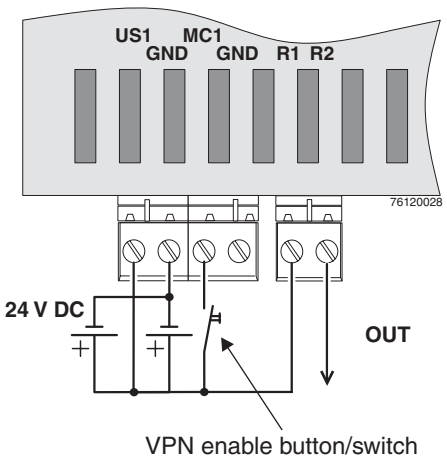


Figure 4-11 Redundant connection of the supply voltage/signal contact with VPN enable button

4.4.3 Connecting to the network

WARNING:

Only connect the FL MGUARD network ports to LAN installations.

When connecting to the network, use cables with bend protection on the connectors.

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

LAN port

- Connect the local computer or the local network to the LAN port of the FL MGUARD using a UTP Ethernet cable (CAT5) or using SFP plug-in modules (optional, see “Ordering data” on page 9-9). **If your computer is already connected to a network, patch the** FL MGUARD **between the existing network connection.**

Please note that configuration can only be completed via the LAN interface and that the firewall of the FL MGUARD GT/GT ... prevents all IP data traffic from the WAN to the LAN interface.

WAN port

- Use a UTP cable (CAT5) or establish the connection using SFP plug-in modules (optional, see “Ordering data” on page 9-9).
- Connect the external network via the WAN female connector, e.g., WAN, Internet. (Connections to the remote device or network are established via this network.)

Driver installation is not required.

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

Functional earth ground

The FL MGUARD GT/GT ... is grounded via the metal housing when it is mounted on a DIN rail. The DIN rail must be grounded.

Signal contact

WARNING: Only SELV circuits with voltage limitations according to EN 60950-1 may be connected to the signal contact.

The signal contact monitors the operation of the FL MGUARD GT/GT ... and thus enables remote diagnostics. Interruption of the contact via the floating signal contact (relay contact, closed current circuit) indicates the following:

– Failure of at least one of the two supply voltages.
– Power supply of the FL MGUARD GT/GT ... below the specified limit value (supply voltage 1 and/or 2 is less than 18 V).
– The faulty link status of at least one port. The link status message for each port can be masked on the FL MGUARD GT/GT ... via the management software.
  By default upon delivery, there is no connection monitoring.
– Error during selftest.

During a restart, the signal contact is interrupted until the FL MGUARD has started up completely. This also applies when the signal contact is manually set to *Closed* in the software configuration.

VPN enable contact

Always supply the VPN enable button from the voltage source that supplies the FL MGUARD GT/GT VPN.

A **button** or an **on/off switch** (e.g., key switch) can be connected to VPN enable contacts **MC1 and** GND.

The **button** or **on/off switch** is used to establish and release a predefined VPN connection. The "INF" LED indicates the status of the VPN connection (see “IPsec VPN >> Global” on page 6-162 under "Options").

Operating a connected button

- To establish the VPN connection, hold down the button for a few seconds until the signal LED flashes. Then release the button.

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

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

Operating a connected on/off switch

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

Signal LED "INF"

If the signal LED 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 signal LED is ON, the VPN connection is present.

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

RS-232 interface for external management

The 6-pos. Mini-DIN female connector provides a serial interface to connect a local management station. It can be used to connect a VT100 terminal or a PC with corresponding terminal emulation to the management interface. Set the following transmission parameters:

Bits per second	38400
Data bits	8
Parity	None
Stop bits	1
Flow control	None

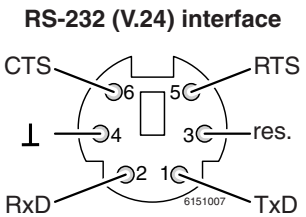


Figure 4-12 Transmission parameters and assignment of the RS-232 interface

4.5 Connecting the FL MGUARD SMART2/ FL MGUARD SMART

Figure 4-13 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.

Only for the power supply (default settings).

The FL MGUARD SMART2 (not the FL MGUARD SMART) can be configured such that a serial consol is available via the USB connector (see Section 6.4.1.5).

WAN port

Female connector for connection to the external network, e.g., WAN, Internet.
(Connections to the remote device or network are established via this network.)

Before:

After:

(A LAN can also be on the left)

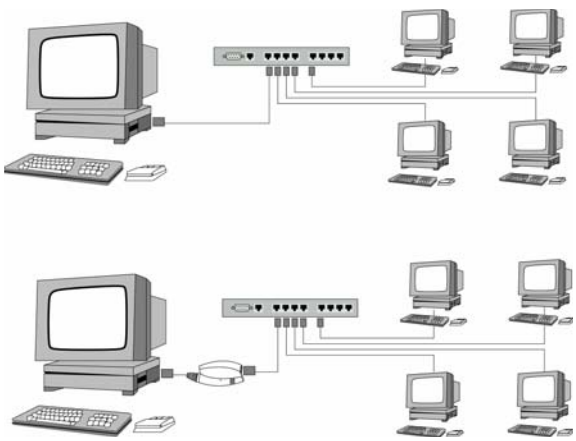


Figure 4-14 FL MGUARD SMART2: Connection to the network**.**

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.

4.6 Installing the FL MGUARD BLADE

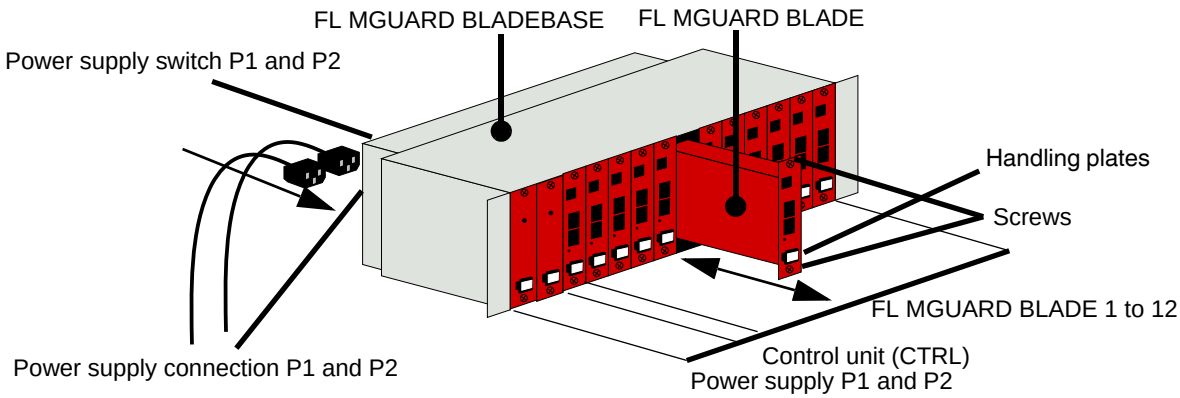


Figure 4-15 Installing the FL MGUARD BLADE

NOTE: Always ensure sufficient air circulation for the BLADEPACK.

If several BLADEPACKS are stacked, one or more inches of fan trays must be installed to discharge the accumulated warm air.

Installing the FL MGUARD BLADEBASE

- Install the FL MGUARD BLADEBASE in the rack, e.g., close to the patch field.
- Fit the two power supply units and the control unit with the handling plates "P1", "P2", and "Ctrl" on the front from left to right.
- Connect both power supply units on the back of the FL MGUARD BLADEBASE with 100 V or 220/240 V.
- Switch on both power supply units.
- The LEDs on the front of the power supply units are now green.

Installing the FL MGUARD BLADE

The FL MGUARD BLADEBASE does not have to be switched off when installing or removing an FL MGUARD BLADE.

- Loosen the top and bottom screw on the faceplate or on the FL MGUARD BLADE to be replaced.
- Remove the faceplate or pull out the old FL MGUARD BLADE.
- Insert the new FL MGUARD BLADE and PCB into the plastic guides and push it completely into the FL MGUARD BLADEBASE.
- Secure the FL MGUARD BLADE by tightening the screws slightly.
- Replace the empty handling plate with the suitable number from the FL MGUARD BLADEBASE accessories, or replace it with the plate from the old FL MGUARD BLADE. To do this, pull or push the plate sideways.

Control unit (CTRL slot)

The CTRL slot is located right next to the two power supply units. An FL MGUARD BLADE operated in this slot acts as the controller (control unit) for all other FL MGUARD BLADE devices.

During initial installation of an FL MGUARD BLADE in the CTRL slot, the BLADE is reconfigured as a control unit as follows:

– The user interface is reconfigured for operation as a controller.
– It switches to router mode with local IP address 192.168.1.1.
– The firewall, CIFS integrity monitoring, and VPN functions are reset and deactivated.

Connecting the FL MGUARD BLADE

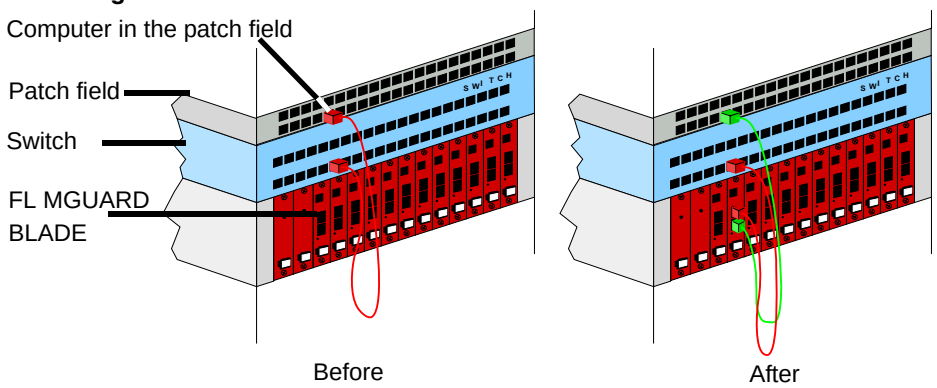


Figure 4-16 Connecting the FL MGUARD BLADE to the network

NOTE: If your computer is already connected to a network, patch the FL MGUARD BLADE between the existing network connection.

Please note that configuration can only be completed from the local computer via the LAN interface and that the firewall of the FL MGUARD prevents all IP data traffic from the WAN to the LAN interface.

Driver installation is not required.

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

Serial port

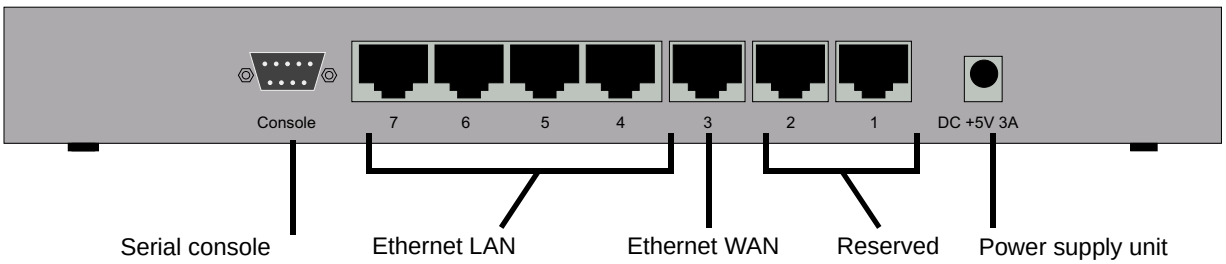
NOTE: The serial interface (RJ12 female connector) must not be connected directly to the telecommunications connections. To connect a serial terminal or a modem, use a serial cable with RJ12 connector. The maximum cable length of the serial cable is 30 m.

The serial port (serial interface) can be used as described in “Serial port” on page 4-10.

4.7 Connecting the FL MGUARD DELTA

WARNING: The serial interface (DE-9 plug-in connection) must not be connected directly to the telecommunications connections. To connect a serial terminal or a modem, use a serial cable with DE-9 connector.

The maximum cable length of the serial cable is 30 m.



Connecting the FL MGUARD DELTA

- Connect the power supply (5 V DC, 3 A) to the "DC +5V, 3A" female connector of the FL MGUARD DELTA.
- Connect the local computer or the local network to one of the Ethernet LAN connections (4 to 7) of the FL MGUARD DELTA using a UTP Ethernet cable (CAT5).

4.8 Installing the FL MGUARD PCI

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: Conditions of acceptability

The device is designed for installation in a PC in the secondary signal circuit and therefore no tests have been performed. The user must evaluate any tests.

The temperature of the PCB must not exceed 105°C.

Selection of driver mode or power-over-PCI mode

There are two operating modes: *driver mode* and *power-over-PCI mode*.

- Before installing it in your PC, decide which mode will be used to operate the FL MGUARD PCI.
- The FL MGUARD PCI is set to the desired mode using a jumper.

Driver mode

The FL MGUARD PCI can be used as a normal network card. This network card then also provides FL MGUARD functions.

In this case, the supplied driver must be installed.

Power-over-PCI mode

If the network card functions of the FL MGUARD are not required or should not be used, the FL MGUARD PCI can be connected after an existing network card (on the same computer or on another) like an FL MGUARD stand-alone device. In this operating mode, the FL MGUARD PCI actually only uses the PCI slot of a computer in order to receive power and as housing. This operating mode of the FL MGUARD is referred to as *power-over-PCI mode*.

A driver is not installed.

4.8.1 Driver mode

In this mode, a driver for the PCI interface of the FL MGUARD PCI (available for Windows XP/2000 and Linux) must be installed later on the computer. In driver mode, no additional network card is required for the computer.

Stealth mode in driver mode (default setting)

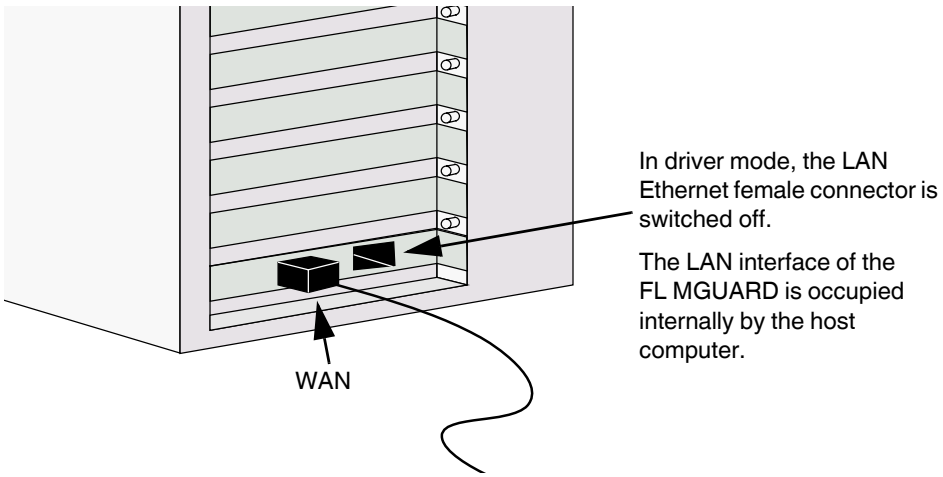


Figure 4-17 Driver mode: Stealth mode

In *stealth* mode, the FL MGUARD behaves like a normal network card.

The IP address that is 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 driver mode

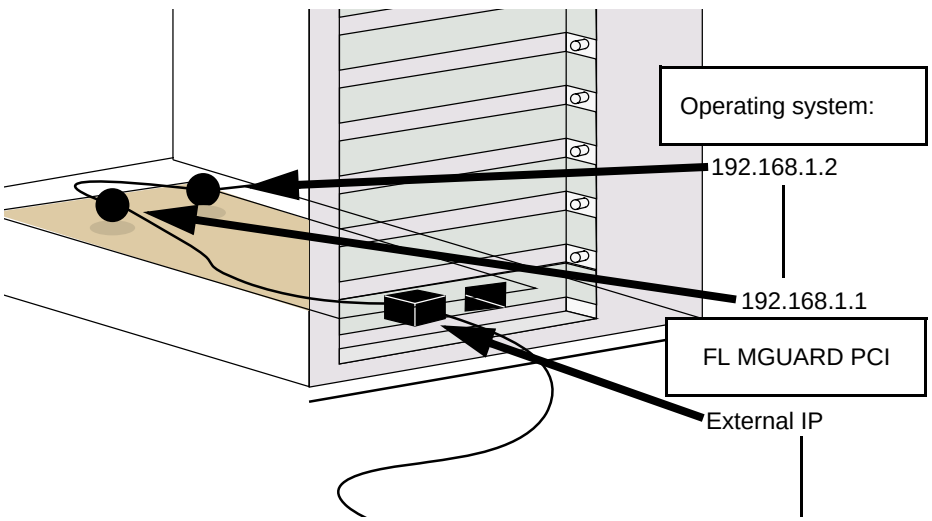


Figure 4-18 Driver mode: Router mode

If the FL MGUARD is in *router* mode (or *PPPoE* or *PPTP* mode), it essentially creates its own network with the operating system of the computer in which the FL MGUARD is installed.

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

(This relationship is shown in the above diagram by two black spheres.)

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).

4.8.2 Power-over-PCI mode

Stealth mode in power-over-PCI mode

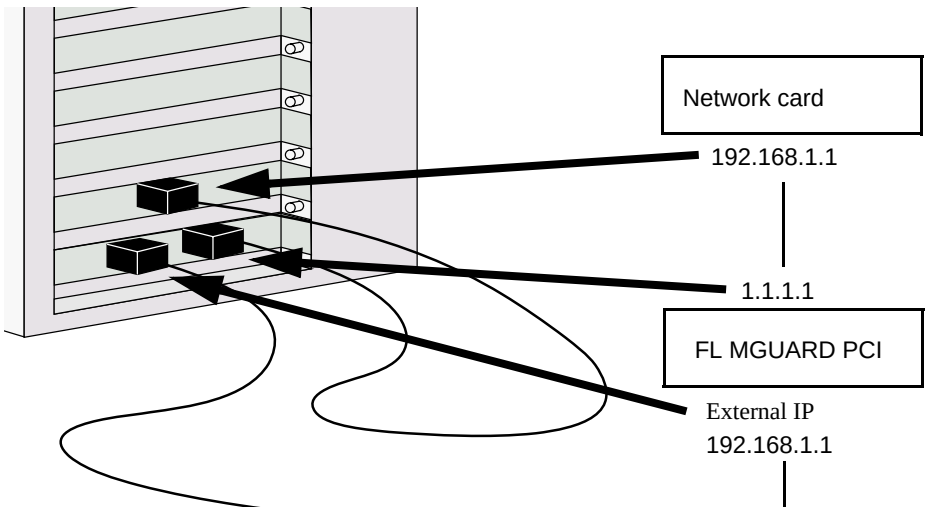


Figure 4-19 Power-over-PCI mode: Stealth mode

Since the network card functions of the FL MGUARD PCI are switched off in power-over-PCI mode, no driver software is installed for it.

A previously installed network card is connected to the LAN port of the FL MGUARD PCI, which is located in the same computer or in another computer (see “Installing the hardware” on page 4-24).

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

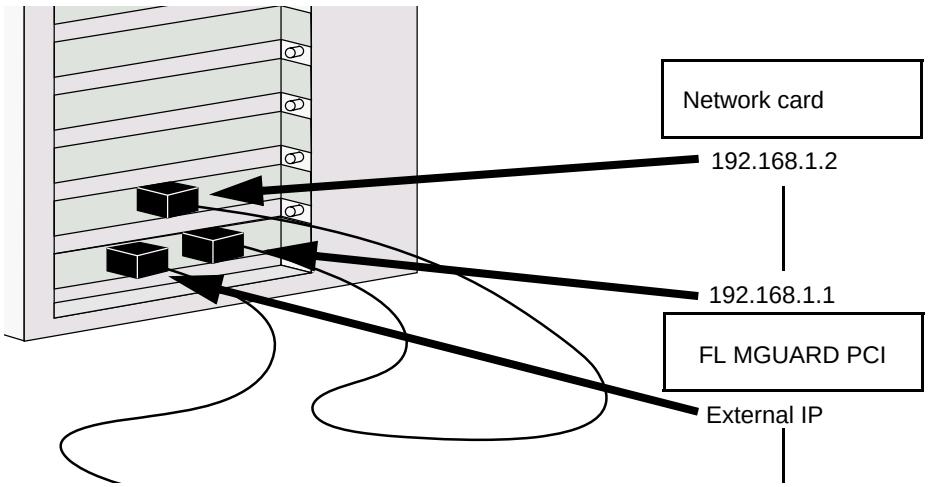


Figure 4-20 Power-over-PCI mode: Router mode

If the FL MGUARD is in *router* mode (or *PPPoE* or *PPTP* mode), the FL MGUARD and the network card connected to its LAN female connector – 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).

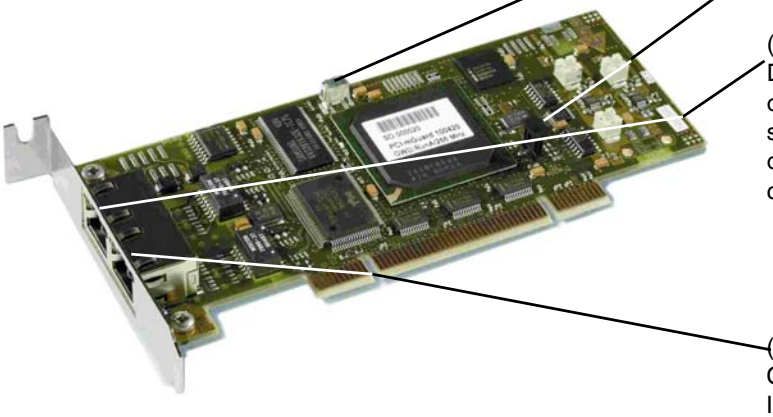
4.8.3 Installing the hardware

NOTE: Electrostatic discharge!

Before installation, touch the metal frame of the PC in which the FL MGUARD PCI is to be installed, in order to remove electrostatic discharge.

The module contains components that can be damaged or destroyed by electrostatic discharge. When handling this module, observe the necessary safety precautions against electrostatic discharge (ESD) in accordance with EN 61340-5-1 and EN 61340-5-2.

FL MGUARD PCI: Structure



(1) Rescue button

(2) Jumper for activating/deactivating driver mode

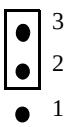
(3) LAN port
Deactivated in driver mode. In power-over-PCI mode, the network card of the same or another computer to be protected or of the network to be protected is connected here.

(4) WAN port
Connections to the external network (e.g., Internet) are established via this interface. With the default firewall settings, incoming connections are blocked here.
Use a UTP cable (CAT5).

How to proceed

- Configure the FL MGUARD PCI for *driver mode* or *power-over-PCI mode* (see “Selection of driver mode or power-over-PCI mode” on page 4-21)
- To do this, set the jumper (2) to the relevant position:

Driver mode



Power-over-PCI mode

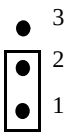


Figure 4-21 Jumper for driver mode or power-over-PCI mode

- Switch off the computer and any other connected I/O devices.
- Observe the safety notes for electrostatic discharge.
- Unplug the power cable.
- Open the computer cover. Please refer to the description in the computer user manual for this step.
- Select a free PCI slot (3.3 V or 5 V) for the FL MGUARD PCI.
- Remove the corresponding slot plate by loosening the relevant screw and pulling out the slot plate.

  Keep the screw for securing the FL MGUARD PCI card.
- Carefully align the male connector of the FL MGUARD PCI card over the female connector of the PCI slot on the motherboard and then press the card evenly into the female connector.

- Tighten the card slot plate.
- Close the computer cover again.
- Connect the computer power cable again and switch on the computer.

4.8.4 Installing the driver

Driver installation is only required and supported if the FL MGUARD PCI is operating in *driver mode* (see “Driver mode” on page 4-21).

Requirements

- If necessary, follow the steps described in “Installing the hardware” on page 4-24.
- You should have the driver files on a data carrier.

If not:

- Download the driver files from the download area at www.innominate.de.
- Extract the files from the ZIP.
- Copy the extracted files to a data carrier, e.g., CD-ROM, USB memory stick.

Under Windows XP

- After installing the hardware, switch on the computer.
- Log on with administrator rights and wait until the following window appears:

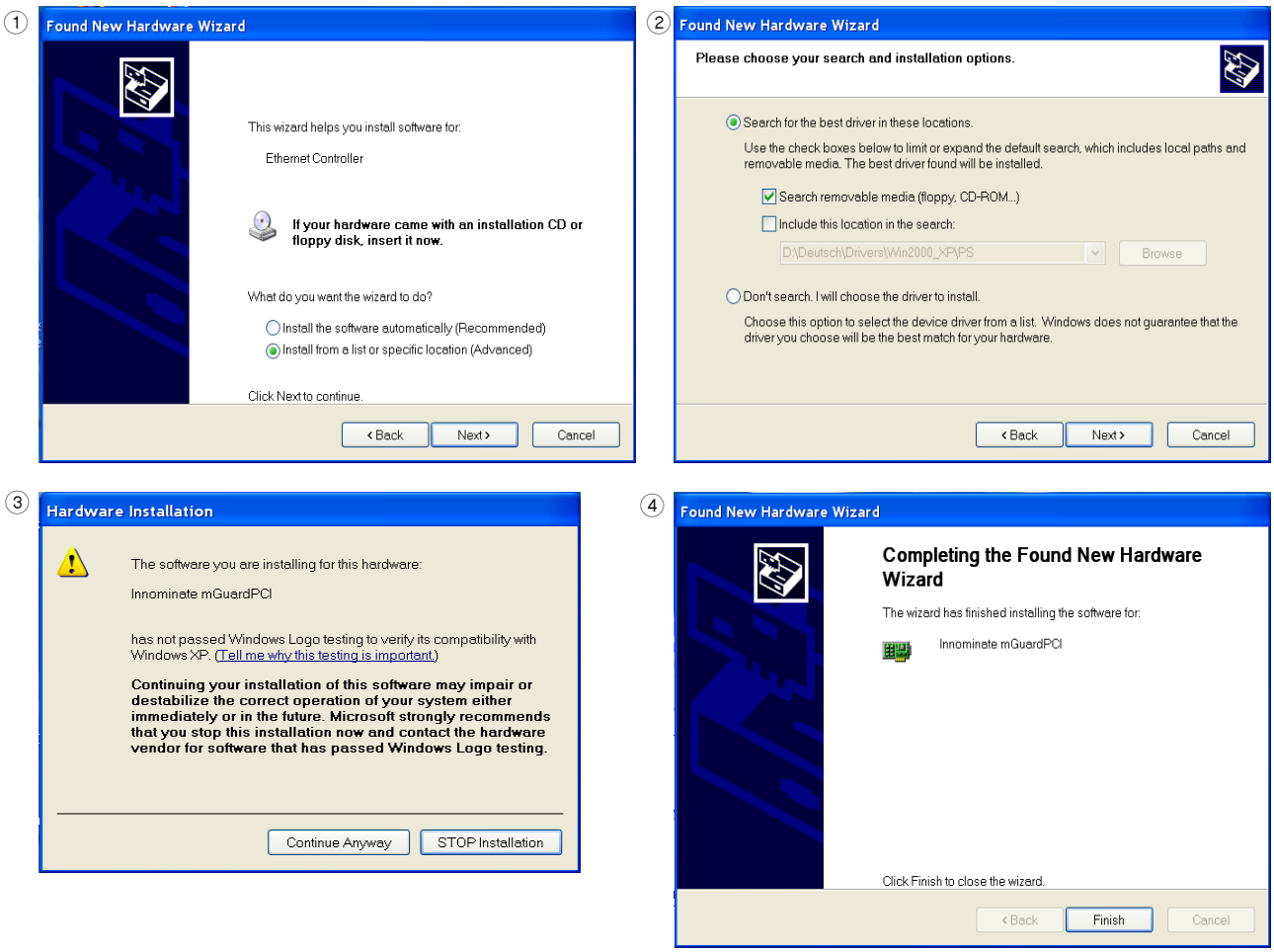


Figure 4-22 Driver installation under Windows XP

1. After inserting the data carrier, select the "Install from a list or specific location (Advanced)" option and click "Next".
2. Click "Next".
3. Click on "Continue Anyway".
4. Click on "Finish".

Under Windows 2000

- After installing the hardware, switch on the computer.
- Log on with administrator rights and wait until the following window appears:

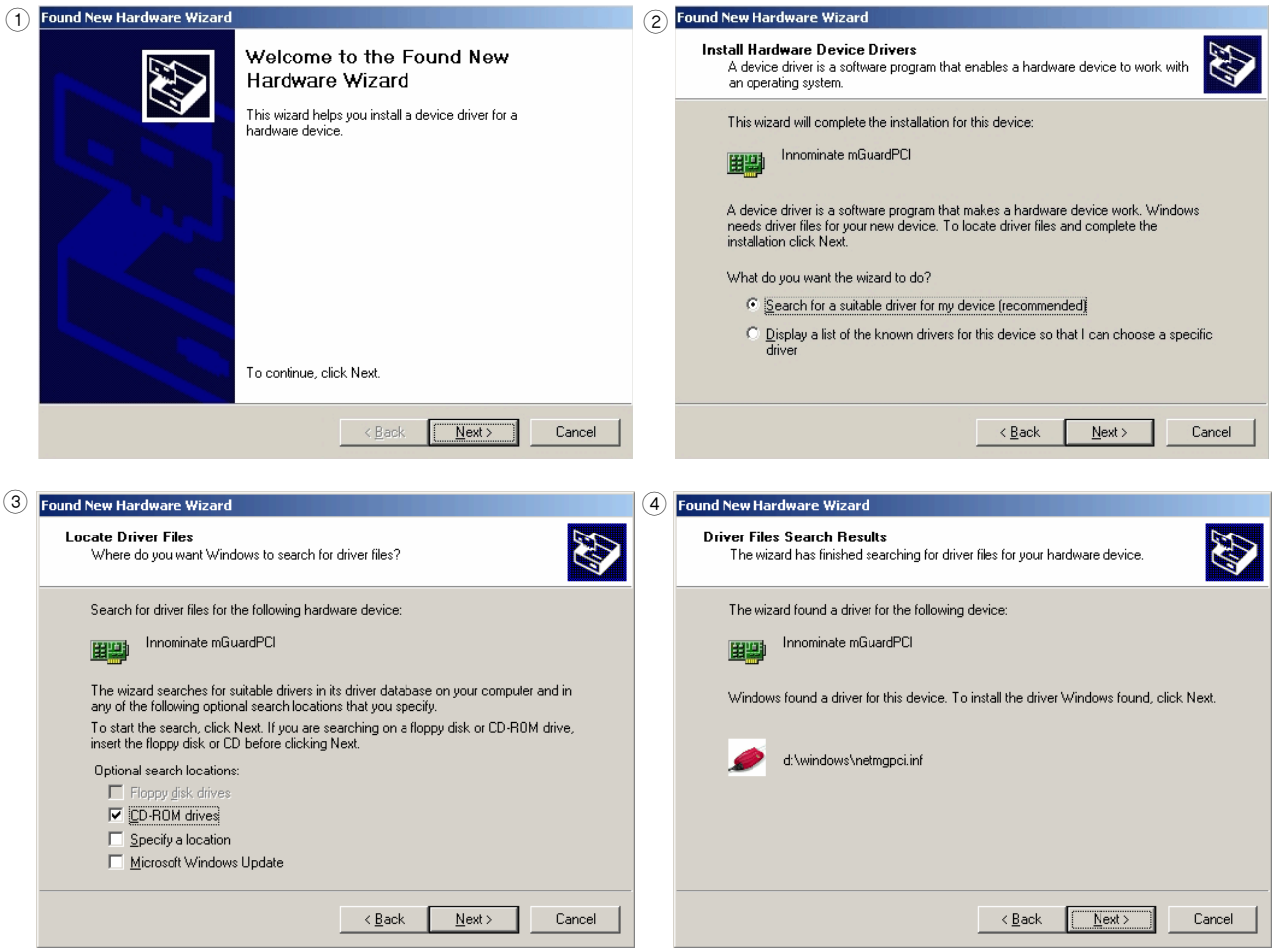


Figure 4-23 Driver installation under Windows 2000 (1)

1. Click "Next".
2. Select "Search for a suitable driver for my device (recommended)" and click "Next".
3. Select "Specify a location" and click "Next".
4. Click "Next".

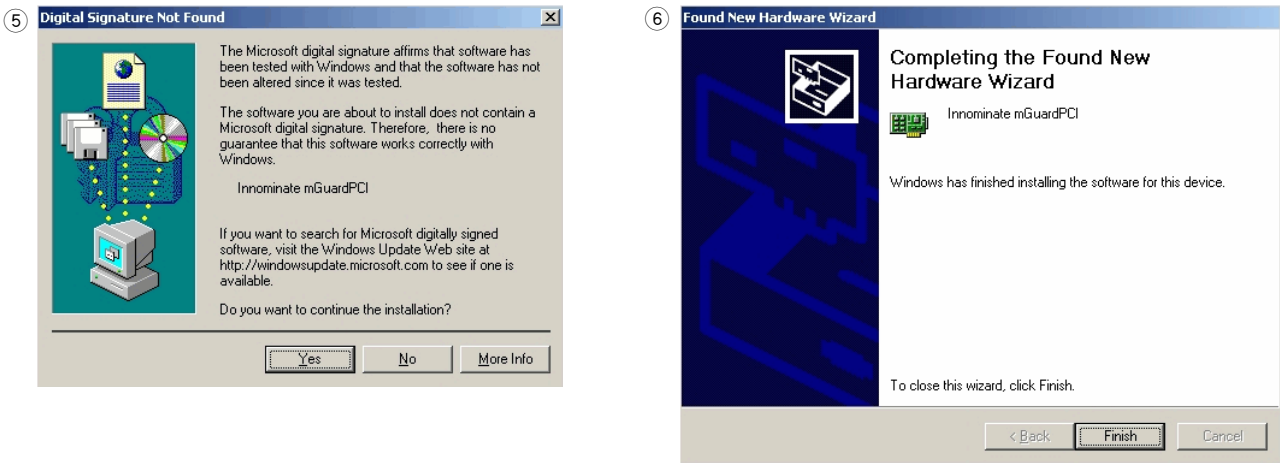


Figure 4-24 Driver installation under Windows 2000 (2)

5. Click "Yes".
6. Click "Finish".

Under Linux

The Linux driver is available in the source code and must be compiled before use:

- First set up and compile the Linux kernel (2.4.25) in the directory /usr/src/linux.
- Extract the drivers from the ZIP to the directory /usr/src/PCI-driver.
- Execute the following commands:

  ```
  cd /usr/src/PCI-driver
  make LINUXDIR=/usr/src/linux
  install -m0644 mguard.o /lib/modules/2.4.25/kernel/drivers/net/
  depmod -a
  ```

- The driver can now be loaded with the following command:
  modprobe mguard

5 Preparing the configuration

5.1 Connection requirements

FL MGUARD RS … / FL MGUARD GT/GT ...

- The FL MGUARD RS .../FL MGUARD GT/GT ... must be connected to at least one active power supply unit.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN female connector 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 SMART2

- The FL MGUARD SMART2 must be switched on, i.e., it must be connected to a computer (or power supply unit) that is switched on via a USB cable in order for it to be supplied with power.
- **For local configuration**: The computer used for configuration:
  - Must be connected to the LAN port of the FL MGUARD
  - Or must be connected to the FL MGUARD 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.

FL MGUARD PCI

- **For local configuration**: The computer used for configuration must meet the following requirements:
  - **FL MGUARD** in *driver mode*: The FL MGUARD PCI driver must be installed on the computer.
  - **FL MGUARD** in *power-over-PCI mode*: 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.

FL MGUARD BLADE

- The FL MGUARD BLADE must be mounted in the FL MGUARD BLADEBASE, and at least one of the BLADEBASE device's power supply units must be in operation.
- **For local configuration**: The computer used for configuration:
  - Must be connected to the LAN female connector of the FL MGUARD
  - Or the computer must be connected to the FL MGUARD via the 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.

FL MGUARD DELTA

- The FL MGUARD DELTA must be connected to its power supply.
- **For local configuration**: The computer used for configuration:
  - Must be connected to the LAN switch (Ethernet female connector 4 to 7) of the FL MGUARD
  - Or must be connected to the FL MGUARD 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.

5.2 Local configuration on startup

The FL MGUARD is configured using a web browser on the computer used for configuration (e.g., MS Internet Explorer Version 6 or later, Mozilla Firefox Version 1.5 or later, Google Chrome, or Apple Safari).

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

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

Table 5-1 Preset addresses

Default settings	Network mode	Management IP #1	Management IP #2
FL MGUARD RS …	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD SMART 2	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD PCI	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD BLADE	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS-B	Router		https://192.168.1.1/
FL MGUARD GT/GT …	Router		https://192.168.1.1/
FL MGUARD BLADE controller	Router		https://192.168.1.1/
FL MGUARD DELTA	Router		https://192.168.1.1/

The configuration on startup is described in two sections:

– For devices provided in "stealth" mode in Section 5.2.1 from page 5-4
– For devices provided in "router" mode in Section 5.2.2 on page 5-9

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

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

– https://192.168.1.1/ (see page 5-4)
– https://1.1.1.1/ (see page 5-5)

Alternatively, an IP address can be assigned via BootP (e.g., using IPAssign.exe) (see “Assigning the IP Address via BootP” on page 5-6).

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

Computers can access the FL MGUARD under 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.

– 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.

For initial configuration of the FL MGUARD PCI, please refer to “Configuring the FL MGUARD on startup” on page 5-10.

5.2.1.1 IP address 192.168.1.1

For devices provided in stealth mode, the FL MGUARD can be accessed via the LAN interface under 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 6-35), 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:

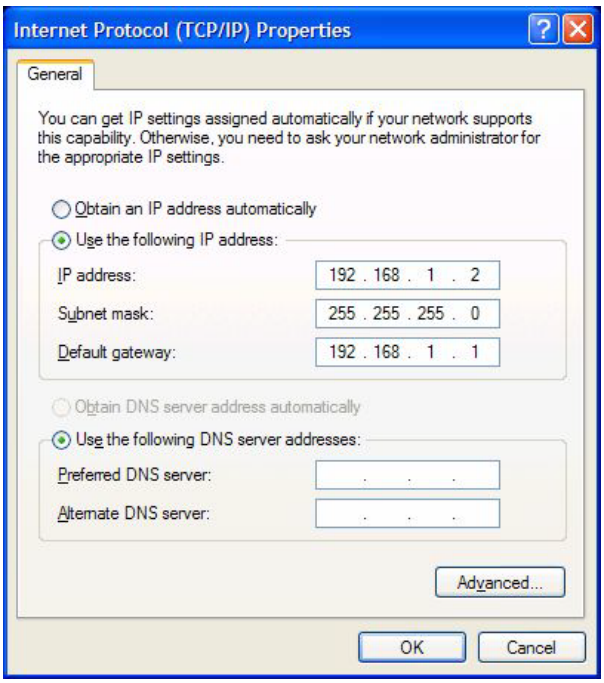


Figure 5-1 Internet Protocol (TCP/IP) Properties

- 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

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.

5.2.1.2 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 4-14 on page 4-17) 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 the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 5-13). Continue from this point.

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

5.2.1.3 Assigning the IP Address via BootP

After assigning an IP address via BootP, the FL MGUARD can no longer be accessed via IP address 192.168.1.1.

For IP address assignment the 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 either be downloaded free if charge at www.phoenixcontact.net/catalog or at www.innominate.de 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 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 www.innominate.de/downloads.
- The Innominate BootP IP addressing tool can be found under "Software & Misc".
- Double-click on "IPAssign_FL MGUARD.exe".
- In the window that opens, click on "Run".

Alternatively, the "IPAssign.exe" tool is also available from Phoenix Contact:

- On the Internet, select the link www.phoenixcontact.net/catalog.
- Enter Order No. 2832700 in the search field, for example.

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

- Double-click on "IPAssign.exe".
- 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.

For reasons of internationality, the program mostly is in English. However, the 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.

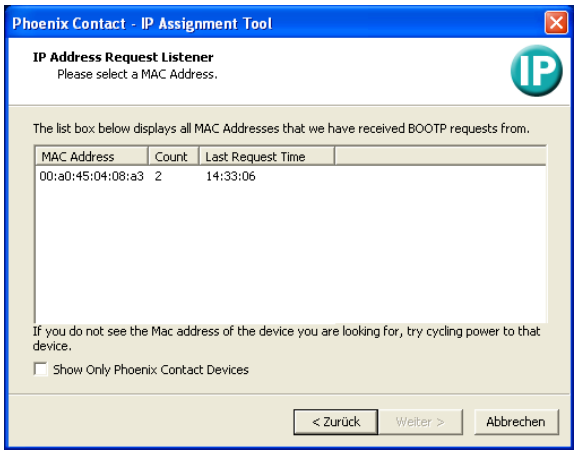


Figure 5-2 "IP Address Request Listener" window

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

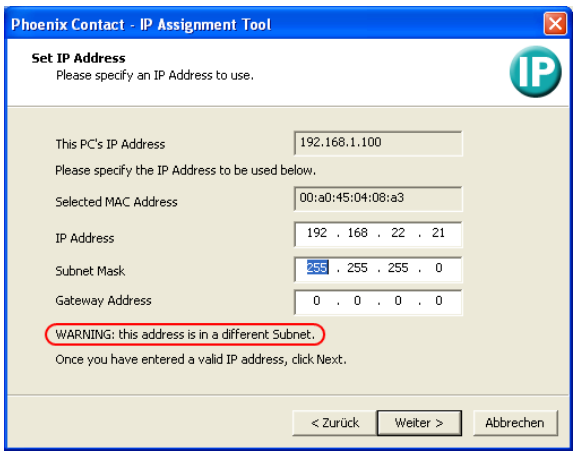


Figure 5-3 "Set IP Address" window with incorrect settings

- 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.

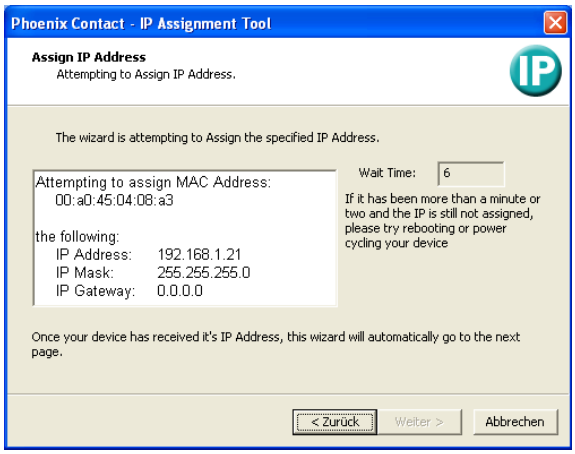


Figure 5-4 "Assign IP Address" window

Following successful transmission, the next window opens.

Step 6: Finishing IP address assignment

The window that opens informs you about successful IP address assignment. It gives an overview of the IP parameters that have been transmitted to the device with the MAC address shown.

For assigning IP parameters for additional devices:

- Click on "Back".

For finishing 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 6-57).

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

FL MGUARD DELTA: By default upon delivery, following reset to the default settings or after flashing the FL MGUARD, the FL MGUARD DELTA can be accessed within the network 192.168.1.0/24 via LAN interfaces 4 to 7 under IP address 192.168.1.1.

FL MGUARD GT/GT ...: By default upon delivery, following reset to the default settings or after flashing the FL MGUARD, the FL MGUARD GT/GT can be accessed within the network 192.168.1.0/24 via the LAN interface under IP address 192.168.1.1.

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

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:

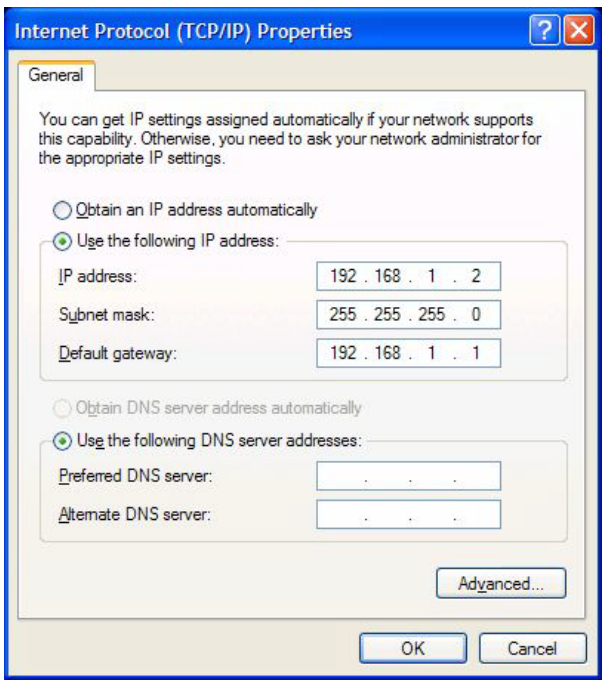


Figure 5-5 Internet Protocol (TCP/IP) Properties

- 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

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.

5.2.3 Configuring the FL MGUARD on startup

Installing the PCI card

- If the PCI card has not yet been installed in your computer, first proceed as described under “Installing the hardware” on page 4-24.

Installing the drivers

- If you have configured the FL MGUARD for **driver mode**, make sure that the drivers are installed as described under “Installing the driver” on page 4-26.

Configuring the network interface

If the FL MGUARD

– Is operated in **driver mode** and the LAN interface (network interface of the computer) has not yet been configured or

– 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:

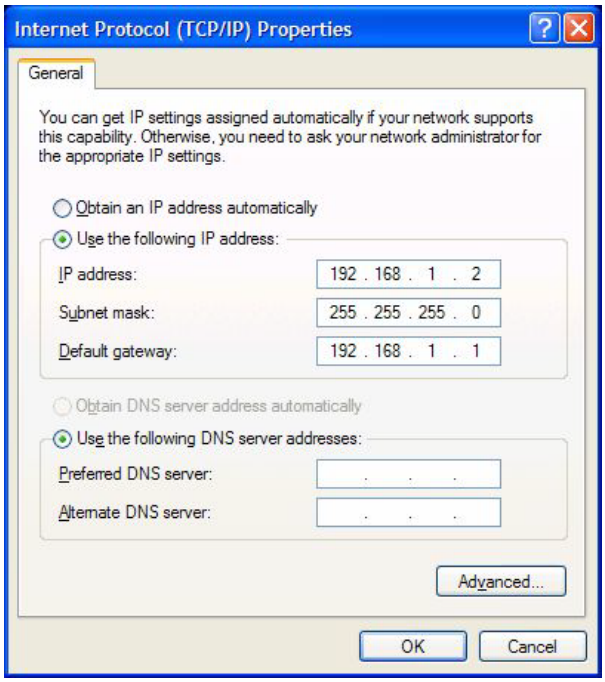


Figure 5-6 Internet Protocol (TCP/IP) Properties

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 5-10 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 5-13).
- 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.

5.3 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 5-2 Preset addresses

Default settings	Network mode	Management IP #1	Management IP #2
FL MGUARD RS …	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD SMART 2	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD PCI	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD BLADE	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS-B	Router		https://192.168.1.1/
FL MGUARD GT/GT …	Router		https://192.168.1.1/
FL MGUARD BLADE controller	Router		https://192.168.1.1/
FL MGUARD DELTA	Router		https://192.168.1.1/
FL MGUARD GT/GT …	Router		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.

With **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 5-2).

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 7-2).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup” on page 5-3).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  With **MS Internet Explorer** (Version 6) 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 5-7 Security alert

Explanation:

As administrative tasks can only be performed when secure (encrypted) access to the device has been established, a self-signed certificate is supplied.

- Click "Yes" to acknowledge the security alert.

The login window is displayed.

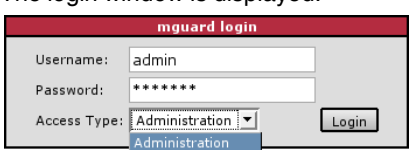


Figure 5-8 Login

- Select the access type – administration or user firewall – and enter your user name and password that are specified for this access type. For user firewall, see “Network Security >> User Firewall” on page 6-144.

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 6-1).

For security reasons, we recommend you change the default root and administrator passwords during initial configuration (see “Authentication >> Local Users” on page 6-111).

5.4 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 6-20 and “Access” on page 6-21) 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 peer:
https://123.45.67.89/

If a different port number is used, it should be entered after the IP address, e.g.,:
https://123.45.67.89:442/

Configuration

- To configure the device, make the desired or necessary settings on the individual pages of the FL MGUARD user interface (see “Configuration” on page 6-1).

6 Configuration

6.1 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 6-1).

– 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.

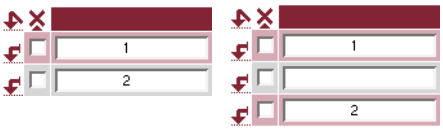
Working with sortable tables

Many settings are saved as data records. Accordingly, the adjustable parameters and their values are presented in the form of table rows. If several data records have been set (e.g., firewall rules), they will be queried or processed based on the order of the entries from top to bottom. 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:

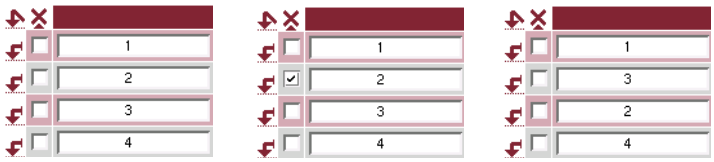
– Insert rows to create a new data record with settings (e.g., the firewall settings for a specific connection)
– Move rows (i.e., resort them)
– Delete rows to delete the entire data record

Inserting rows



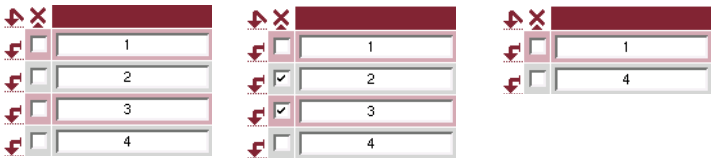
1. Click on the arrow below which you want to insert a new row.
2. The new row is inserted.
   You can now enter or specify values in the row.

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 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:

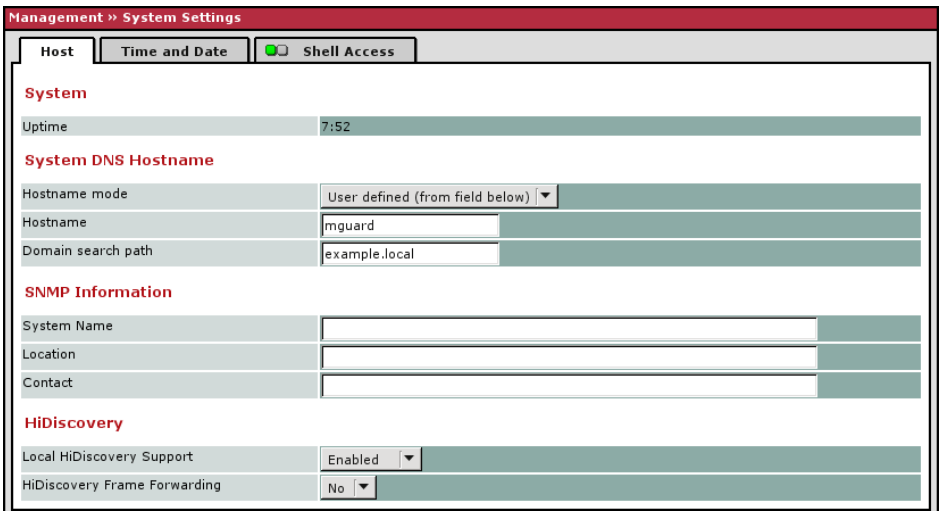
Logout 	For logging out after configuration access to the FL MGUARD. If the user does not log out, he/she is logged out automatically if there has been no further activity and the time period specified by the configuration has elapsed. Access can only be restored by logging in again.
Reset 	Optional 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 6-20).
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 6-20).

6.2 Management menu

For security reasons, we recommend you change the default root and administrator passwords during initial configuration (see “Authentication >> Local Users” on page 6-111). A message informing you of this will continue to be displayed at the top of the page until the passwords are changed.

6.2.1 Management >> System Settings

6.2.1.1 Host

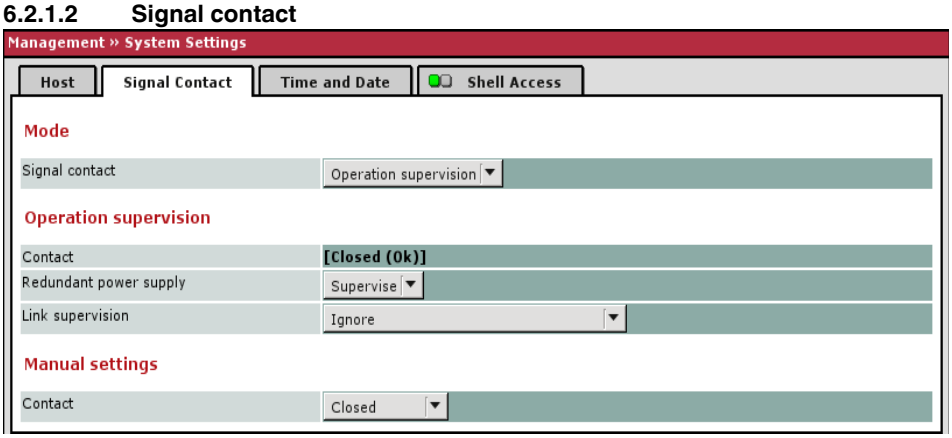


Management >> System Settings >> Host	
System	
	Uptime Device operating time since the last restart.
	(FL MGUARD GT/GT ..., FL MGUARD RS ... only)
	Power supply 1/2 State of both power supply units.
	Temperature (°C) An SNMP trap is triggered if the temperature exceeds or falls below the specified temperature range.

Management >> System Settings >> Host (Fortsetzung)		
System DNS Hostname	**Hostname mode**	You can assign a name to the FL MGUARD using the *Hostname mode* and *Hostname* fields. For example, this name is then displayed when logging in via SSH (see “Management >> System Settings” on page 6-4, “Shell Access” on page 6-11). 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 includes the phone number (under SNMP: sysContact).
HiDiscovery		HiDiscovery is a protocol that supports the initial startup of new network devices and is available in *stealth* mode for the local interface (LAN) of the FL MGUARD.

Management >> System Settings >> Host (Fortsetzung)		
	Local HiDiscovery support	**Enabled** The HiDiscovery protocol is activated. **Read only** The HiDiscovery protocol is activated, but it cannot be used to configure the FL MGUARD. **Disabled** The HiDiscovery protocol is deactivated.
	HiDiscovery Frame Forwarding: Yes/No	If this option is set to **Yes**, then HiDiscovery frames are forwarded from the LAN port externally via the WAN port.

6.2.1.2 Signal contact



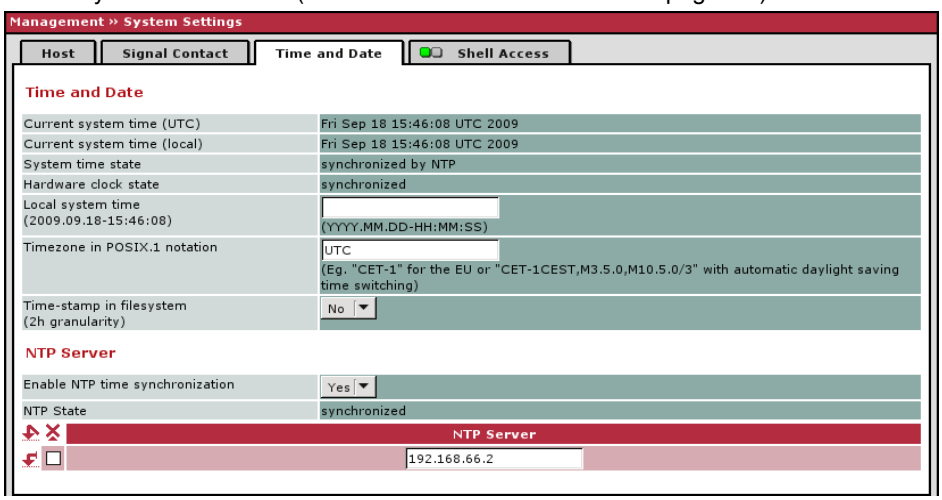
The signal contact is a relay that is used by the FL MGUARD to signal error states (see also “Signal contact” on page 4-8)

Management >> System Settings >> Signal Contact		
Mode	(FL MGUARD RS ... , FL MGUARD GT/GT... only)	
	Signal contact	The signal contact can be controlled automatically using **Operation supervision** (default) or **Manual settings**. See also: “Installing the FL MGUARD RS ...” on page 4-4 and “Connecting the FL MGUARD DELTA” on page 4-20.
Operation supervision	**Contact**	Displays the status 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 power supply voltages fails.

Management >> System Settings >> Signal Contact (Fortsetzung)		
	Link supervision	Monitoring of the link status of the Ethernet connections. Possible settings are: – Ignore – Supervise internal only (trusted) – Supervise external only (trusted) – Supervise both
Manual settings	**Contact**	If **Signal contact** has been set to **Manual settings**, the contact can be set to **Closed** or **Open (Alarm)** here.

6.2.1.3 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 6-8).



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)	Indication: 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	Indication: Indicates whether the FL MGUARD system time and run time have ever actually been synchronized with a valid time. If 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 (Fortsetzung)

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 6-35, “Configuration Pull” on page 6-49).

– **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 6.4.1“Network >> Interfaces”, ““Router" network mode, "PPPoE" router mode” on page 6-78).

– **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 6.5.3 and “Certificate settings” on page 6-121).

– **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** option 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 then 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 (Fortsetzung)

Hardware clock state

(For *FL MGUARD RS ...*, *FL MGUARD DELTA, FL MGUARD GT/GT ...*, and for *FL MGUARD SMART2*, but not for *FL MGUARD SMART*)

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 status only returns to "not synchronized" if the firmware is reinstalled on the device (see Section 7.3, “Flashing the firmware/rescue procedure”) or if the capacitor (FL MGUARD RS ...) or the battery (FL MGUARD DELTA) 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
mm	Minute
ss	Second

Timezone in POSIX.1 notation...

If a current local time (that differs from Greenwich Mean Time) should 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.

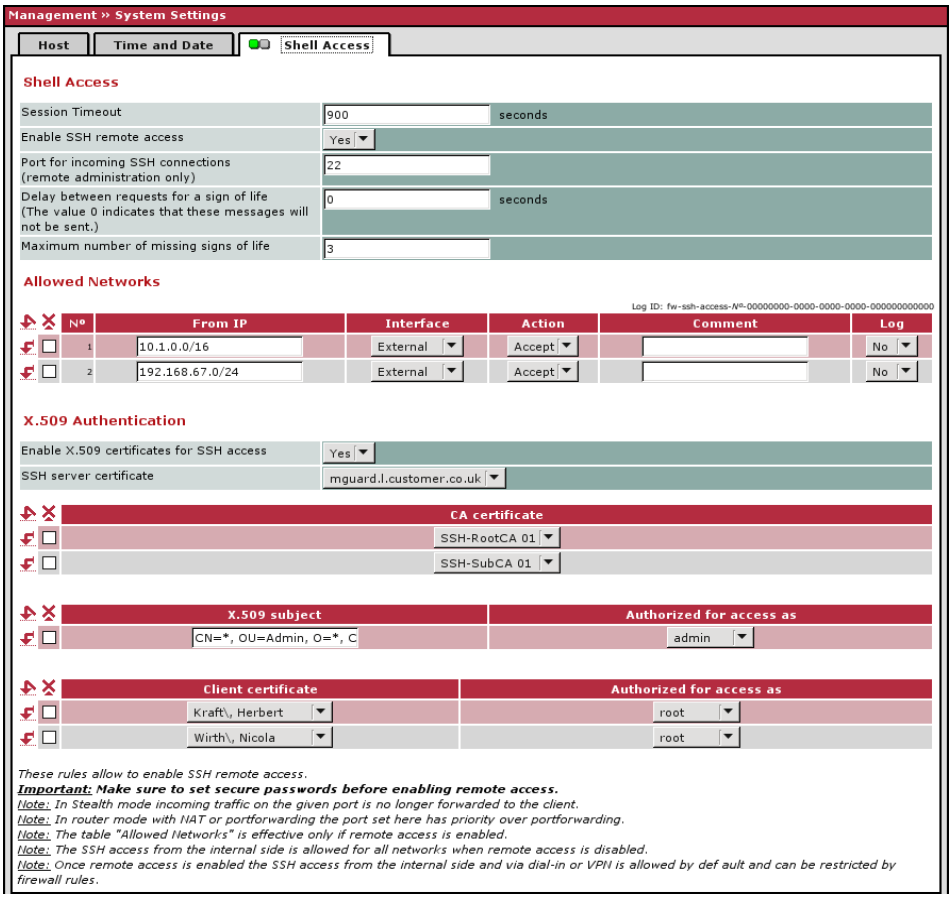
The only important thing is the -1, -2 or +1, etc. value as only these are evaluated – not the preceding letters. They can be substituted with "CET" or any other designation, such as "UTC".

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 (Fortsetzung)		
	Time-stamp in filesystem (2h granularity): Yes/No	If this option is set to **Yes**, the FL MGUARD will write 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 "clock" 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 RS ..., FL MGUARD DELTA, FL MGUARD GT/GT ... and FL MGUARD SMART 2, not FL MGUARD SMART*). 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 (Fortsetzung)	
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.

6.2.1.4 Shell Access



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

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:

Management >> System Settings >> Shell Access (Fortsetzung)		
	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 effect 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 correct functioning of the connection is no longer provided, see “Delay between requests for a sign of life” on page 6-13.
	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)	Default: 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 peer 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 peer. 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 (Fortsetzung)

Delay between requests for a sign of life

The preset "0" means that no requests for a sign of life are sent.

Positive values from 1 to 3600 can be set. They indicate that the FL MGUARD sends a request to the remote peer within the encrypted SSH connection to find out whether it can be accessed. The request is sent, if no activity was detected from the remote peer for the specified number of seconds (e.g., due to network traffic within the encrypted connection).

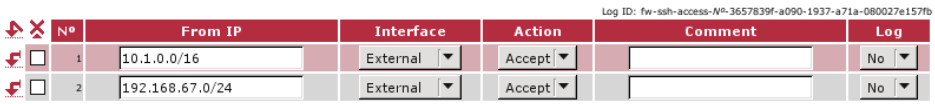
The value entered relates to the functionality of the encrypted SSH connection. As long as the functions are working properly, the SSH connection is not terminated by the FL MGUARD as a result of this setting, even when the user does not perform any actions during this time.

Maximum number of missing signs of life

Specifies the maximum number of times a sign of life request to the remote peer 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 SSH connection is deleted when a sign of life is not detected after approximately 45 seconds.

Allowed Networks



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.

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 IP addresses. To specify an address area, use CIDR format, see “CIDR (Classless Inter-Domain Routing)” on page 6-220.

Management >> System Settings >> Shell Access (Fortsetzung)

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 6-57.

Specifies to which interface the rules 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 simultaneously permit access via another interface explicitly with *Accept* before the new setting takes effect by clicking on the **Apply** button. 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, so the sender is informed of their rejection. (In *stealth* mode, *Reject* has the same effect as *Drop*.)
- **Drop** means that the data packets may not pass through. They are discarded, which means that the sender is not informed of their whereabouts.

Comment

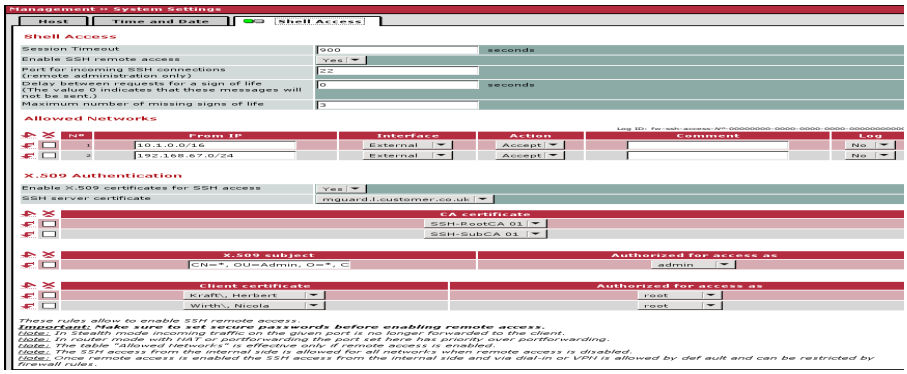
Freely selectable comment for this rule.

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)

X.509 Authentication



Management >> System Settings >> Shell Access		
X.509 Authentication	**Enable X.509 certificates for SSH access: Yes/No**	– 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 is thus compatible with 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 6-116).

Management >> System Settings >> Shell Access (Fortsetzung)

SSH server certificate (2)

Specifies how the FL MGUARD authenticates the SSH client.

The following definition relates to how the FL MGUARD verifies the authentication 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 6.5.3, “Authentication >> Certificates”.

Authentication for SSH

The remote peer shows the following:	Certificate (specific to individual) **signed by CA**	Certificate (specific to individual), **self-signed**
The FL MGUARD authenticates the remote peer using:		
	All CA certificates that form the chain to the root CA certificate together with the certificate shown by the remote peer 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 6.5.3, “Authentication >> Certificates”).

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 SSH client must be 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.

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 (see glossary under *“Subject, certificate” on page 8-5*)

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

Management >> System Settings >> Shell Access (Fortsetzung)

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.
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.

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.

Several filters can be set and their sequence is irrelevant.

Authorized for access as

All users/root/admin/netadmin/audit

Additional filter which defines 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.

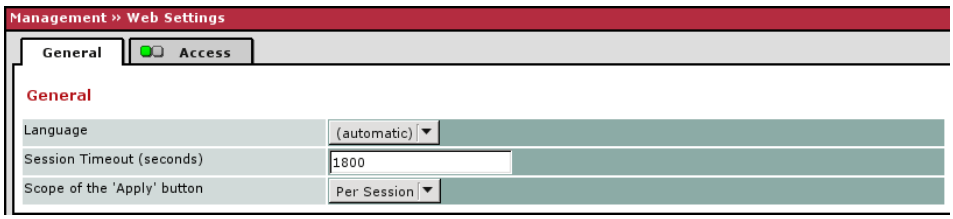
The *netadmin* and *audit* setting options relate to access rights with the Innominate Device Manager.

Management >> System Settings >> Shell Access (Fortsetzung)

Client certificate	This 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 remote peer (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 defines 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. The *netadmin* and *audit* setting options relate to access rights with the Innominate Device Manager.

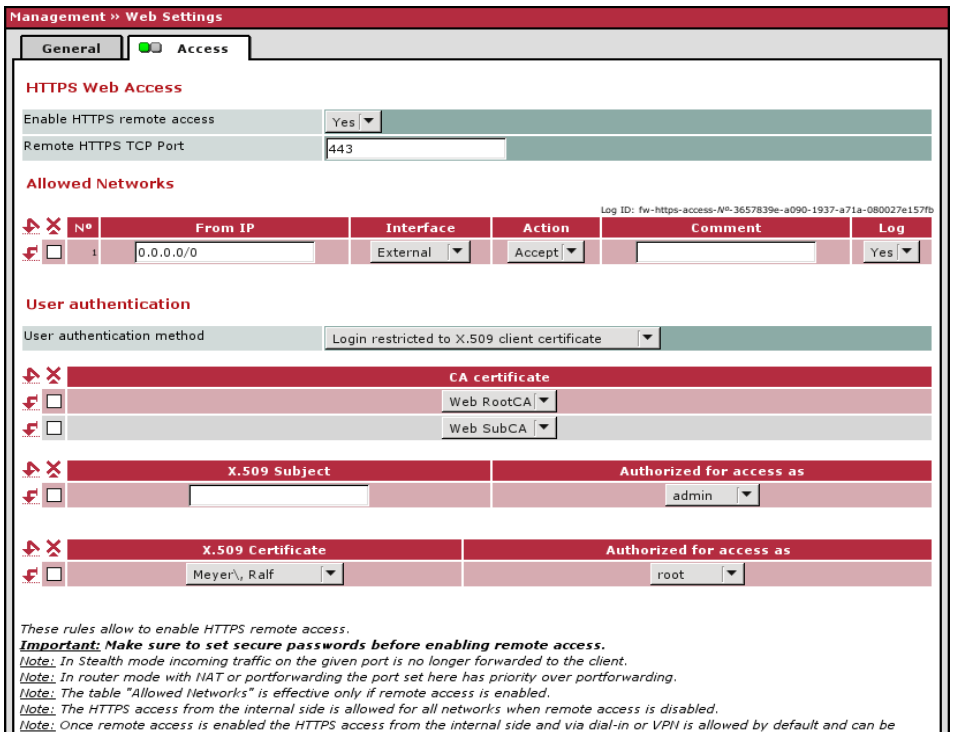
6.2.2 Management >> Web Settings

6.2.2.1 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.

6.2.2.2 Access



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

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.

Management >> Web Settings >> Access (Fortsetzung)

Remote HTTPS TCP Port

Default: 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 peer that implements remote access may have to specify the port number defined here after the IP address during entry of the address.

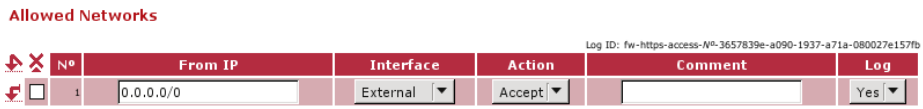
Example:

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 peer.

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 remote peer, 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.

Allowed Networks



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 IP addresses. To specify an address area, use CIDR format – see “CIDR (Classless Inter-Domain Routing)” on page 6-220.

Management >> Web Settings >> Access (Fortsetzung)

Interface

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

Specifies to which interface the rules 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.

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 simultaneously permit access via another interface explicitly with *Accept* before the new setting takes effect by clicking on the **Apply** button. 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, so the sender is informed of their rejection. (In *stealth* mode, *Reject* has the same effect as *Drop*.)
- **Drop** means that the data packets may not pass through. They are discarded, which means that the sender is not informed of their whereabouts.

Comment

Freely selectable comment for this rule.

Log

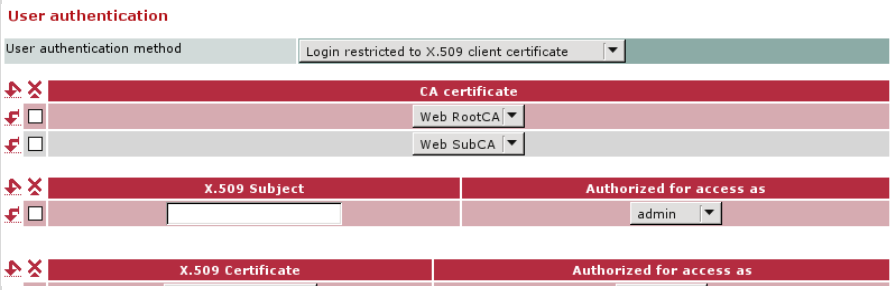
For each individual firewall rule, you can specify whether the use of the rule:

- 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 6-57).

Management >> Web Settings >> Access

User authentication



Defines how the local FL MGUARD authenticates the remote peer

User authentication method

Login with password

Specifies that the remote FL MGUARD user must use a password to log in to the FL MGUARD. The password is specified under the *Authentication >> Local Users* menu (see page 6-111).

Depending on which user ID is used (user or administrator password), the user has the corresponding rights to operate and configure the FL MGUARD.

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 here.

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.

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 6-116.

X.509 authentication for HTTPS

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

1 The remote peer 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 6-116).

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 client 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.

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**.

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 (see glossary under “Subject, certificate” on page 8-5)

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 browser/HTTPS client are permitted. It is then no longer necessary to identify or define the subject in the certificate.

Management >> Web Settings >> Access (Fortsetzung)

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.
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.

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.

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").

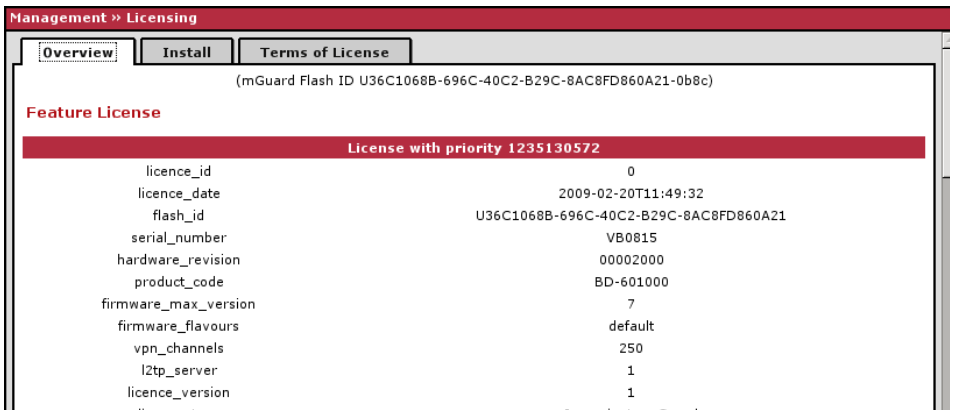
This has the following result: If there are several filters that "let through" a certain user, then the first filter applies. The user is assigned the access rights as defined by this filter. This could differ from the access rights assigned to the user in the subsequent filters.

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 (Fortsetzung)		
	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 >> Local Users” on page 6-111. The *netadmin* and *audit* authorization levels relate to access rights with the Innominate Device Manager.
	X.509 Certificate	This 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 remote peer (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 >> Local Users” on page 6-111. The *netadmin* and *audit* authorization levels relate to access rights with the Innominate Device Manager.

6.2.3 Management >> Licensing

6.2.3.1 Overview

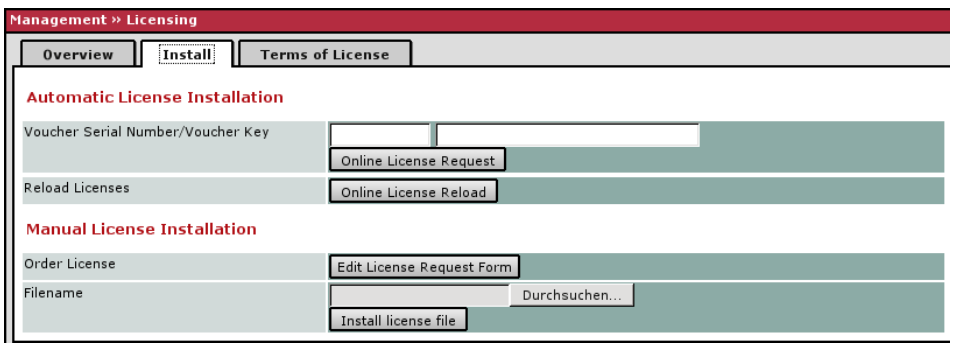


With FL MGUARD Version 5.0 or later, licenses remain installed even after the firmware is flashed.
However, licenses are still deleted when devices with older firmware versions are flashed to Version 5.0.0 or later. Before flashing, the license for using the new update must first be obtained so that 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 7-3).

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.

6.2.3.2 Install

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



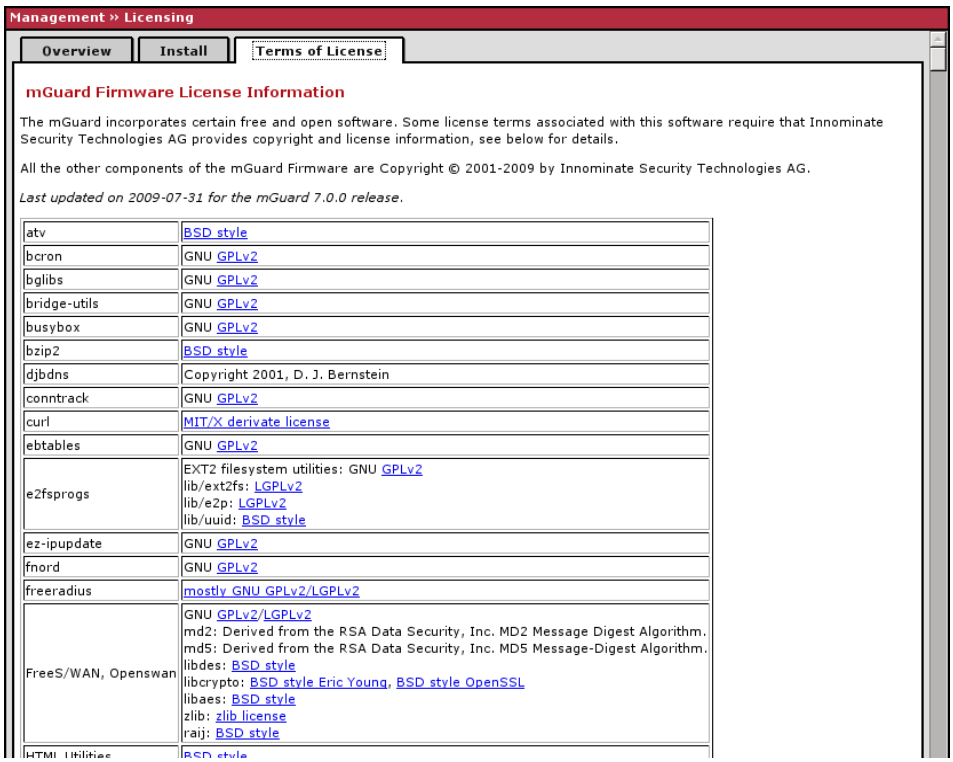
find a voucher serial number and a voucher key in the voucher included with the FL MGUARD. The voucher can also be purchased separately.

It can be used to:

– Request the required feature license file
– Install the license file

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 separate 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**.

6.2.3.3 Terms of License



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

6.2.4 Management >> Update

With FL MGUARD firmware Version 5.0.0 or later, a license must be obtained for the relevant device before a major release upgrade (e.g., from Version 4.x.y to Version 5.x.y or from Version 5.x.y to Version 6.x.y) can be installed.

The license must be installed on the device before updating the firmware (see “Management >> Licensing” on page 6-29 and “Install” on page 6-29).

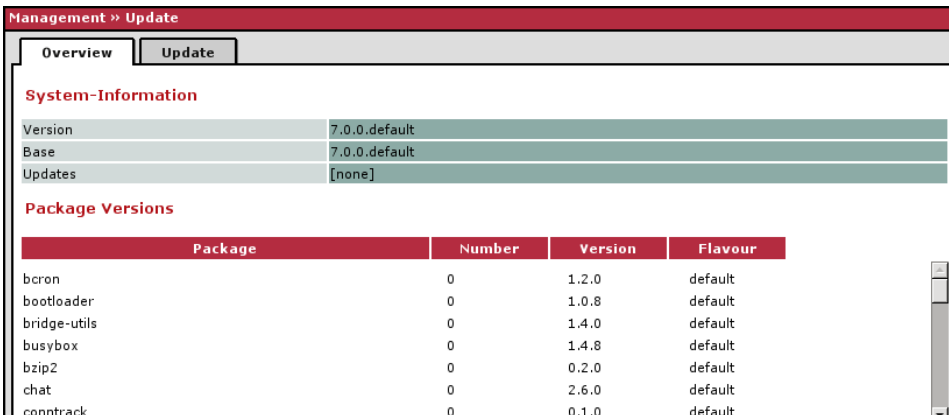
Minor release upgrades (i.e., the same major version, e.g., within Version 5.x.y) can be installed without a license until further notice.

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

The "Firewall Redundancy" function is not available in firmware Version 7.2.

Devices with an installed license for firewall redundancy reject firmware updates to Version 7.2 if the "Firewall Redundancy" function is activated.

6.2.4.1 Overview

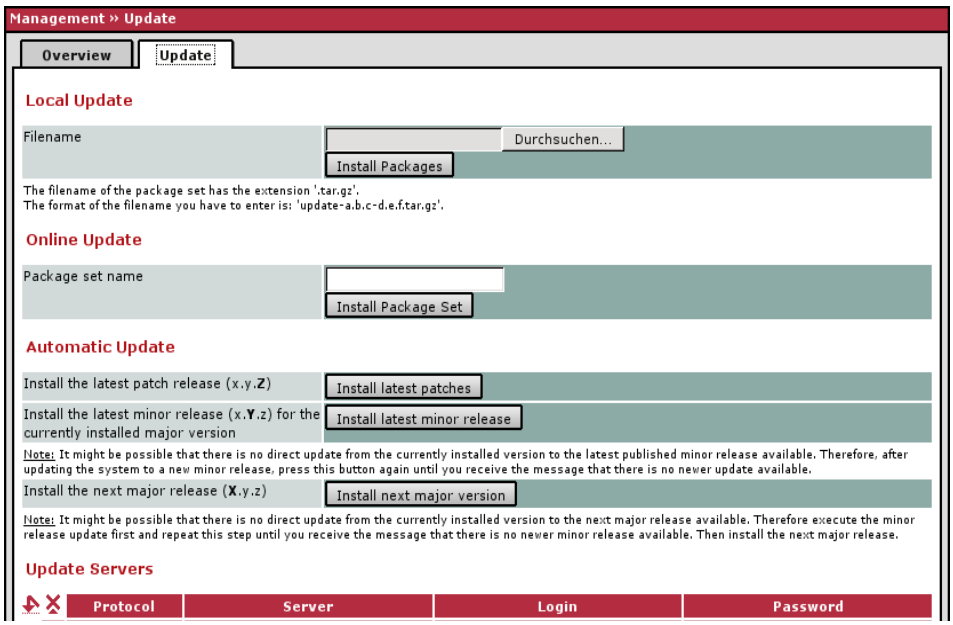


Management >> Update >> Overview		
System Information	**Version**	The current software version of the FL MGUARD.
	Base	The software version that was originally used to flash this FL MGUARD.
	Updates	List of updates that have been installed on the base.
Package Versions	Lists the individual software modules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

6.2.4.2 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. You download the package set file via the Internet from the update server and then install the packages.



NOTE: Do not interrupt the power supply to the FL MGUARD during the update process. 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.

With FL MGUARD firmware Version 5.0.0 or later, a license must be obtained for the relevant device before a major release upgrade (e.g., from Version 4.x.y to Version 5.x.y or from Version 5.x.y to Version 6.x.y) can be installed.

The license must be installed on the device before updating the firmware (see “Management >> Licensing” on page 6-29 and “Install” on page 6-29).

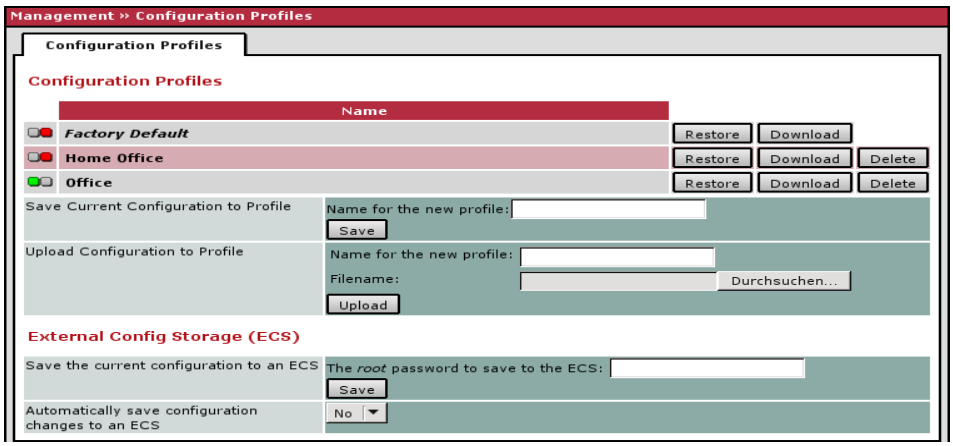
Minor release upgrades (i.e., the same major version, e.g., within Version 5.x.y) can be installed without a license until further notice.

The "Firewall Redundancy" function is not available in firmware Version 7.2. Devices with an installed license for firewall redundancy reject firmware updates to Version 7.2 if the "Firewall Redundancy" function is activated.

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.
	Login	Login for the server.
	Password	Password for login.

6.2.5 Management >> Configuration Profiles

6.2.5.1 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, 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.

For the FL MGUARD GT/GT ... the configuration profiles can also be stored on an external configuration memory (MEM PLUG) which can be connected to the M12 female connector of the FL MGUARD.

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

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

Management >> Configuration Profiles (Fortsetzung)

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.
  (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.

The *Factory Default* profile cannot be deleted.

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.

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 (MEM PLUG)

Save the current configuration to an MEM PLUG

For FL MGUARD GT/GT ... only

When replacing the original device with a replacement device, the configuration profile can be applied using the MEM PLUG. 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", the other password must be entered in the **The root password to save to the MEM PLUG** field.

Management >> Configuration Profiles (Fortsetzung)

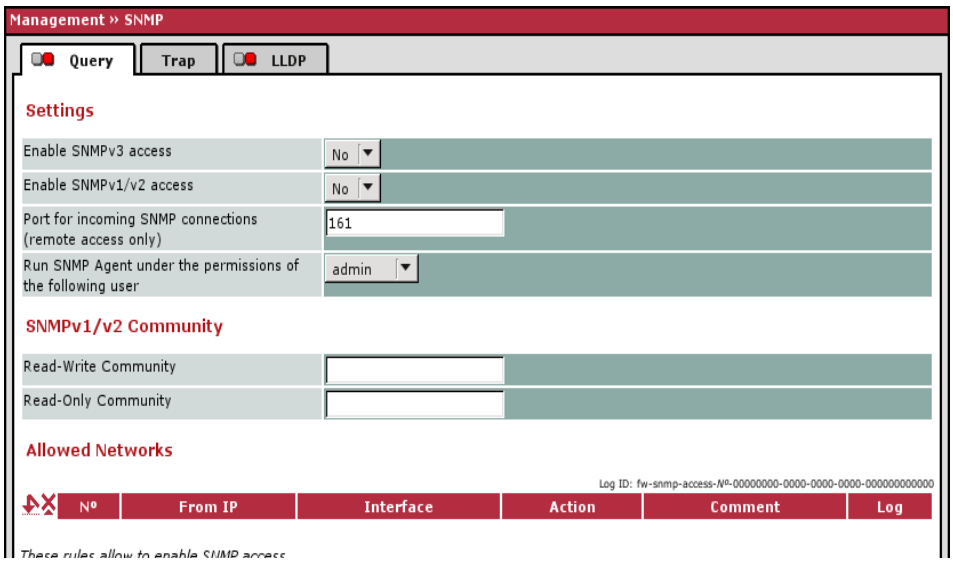
Automatically save configuration changes to an MEM PLUG	*For FL MGUARD GT/GT ... only* When set to **Yes**, the configuration changes are automatically saved to the MEM PLUG, i.e., the MEM PLUG always stores the profile currently used. The FL MGUARD only uses the automatically stored configuration profiles upon startup, if the original password ("root") is still set on the FL MGUARD for the "root" user. Configuration changes are also made, if the MEM PLUG is disconnected, full, or defective. The corresponding error messages are displayed in the Logging menu (see Section 6.12.2). Activation of the new settings extends the response time of the user interface when changing any settings.

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.

6.2.6 Management >> SNMP

6.2.6.1 Query



The SNMP (Simple Network Management Protocol) is mainly used in more complex networks to monitor the status 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. It is therefore not recommended that SNMPv1/SNMPv2 is used.

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

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.

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.

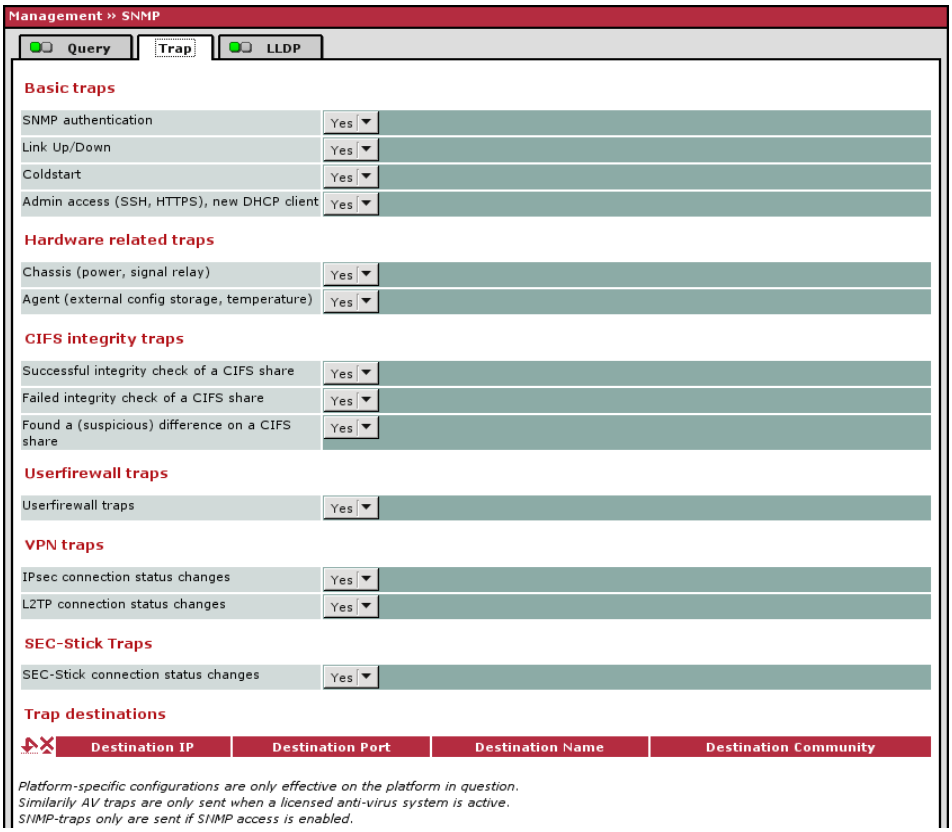
Management >> SNMP >> Query		
Settings	**Enable SNMPv3 access: Yes/No**	If you wish to allow monitoring of the FL MGUARD via SNMPv3, set this option to **Yes**. The firewall rules for the available interfaces must be defined on this page under **Allowed Networks** in order to specify differentiated access 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	Default: 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 peer 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 (Fortsetzung)

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 6-220) – **0.0.0.0/0** means all addresses.
Interface	**External/Internal/External 2/VPN/Dial-in**[1] Specifies to which interface the rules 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 simultaneously permit access via another interface explicitly with *Accept* before the new setting takes effect by clicking on the **Apply** button. 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, so the sender is informed of their rejection. (In *stealth* mode, *Reject* has the same effect as *Drop*.) **Drop** means that the data packets may not 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 6-57).

6.2.6.2 Trap



In certain cases, the FL MGUARD can send SNMP traps.

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.

If SNMP traps are sent to the remote peer via a VPN channel, the IP address of the remote peer 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 6-172).

– 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 6-180), 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 6-180), 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 port, the value is 0.0.0.0. – 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.

Management >> SNMP >> Trap (Fortsetzung)		
		– 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 RS ... only)	**Chassis (power, signal relay)**	Activate traps **Yes/No** – enterprise-oid : FL MGUARDTrapSenderRS ... – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapRS ...PowerStatus (2) – additional : FL MGUARDTrapRS ...PowerStatus Sent when the system registers a power failure. – enterprise-oid : FL MGUARDTrapSenderRS ... – 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).
	Agent (external config storage, temperature)	Activate traps **Yes/No** – enterprise-oid : FL MGUARDTrapRS ... – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapRS ...Temperature (1) – additional : FL MGUARDSystemTemperature, FL MGUARDTrapRS ...TempHiLimit, FL MGUARDTrapRS ...LowLimit The trap indicates the temperature in the event the temperature exceeds the specified limit values.

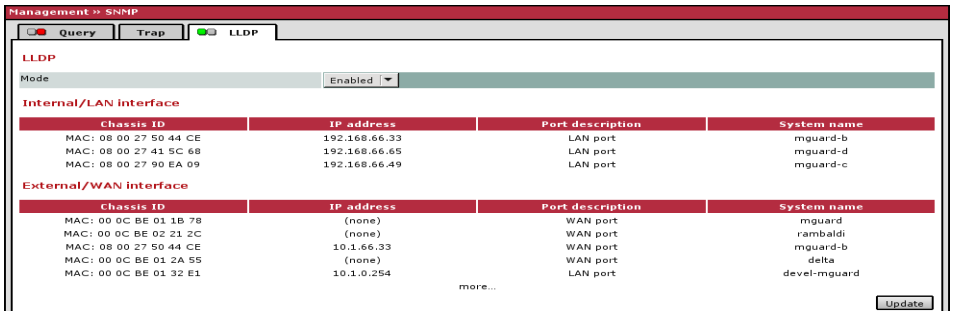
Management >> SNMP >> Trap (Fortsetzung)		
		– enterprise-oid : FL MGUARDTrapRS ... – genericTrap : enterpriseSpecific – specific-trap : FL MGUARDTrapAutoConfigAdapterState (4) – additional : FL MGUARDTrapAutoConfigAdapter Change This trap is sent after access to the ECS.
FL MGUARD BLADE controller traps (BLADE only)	**Blade status change**	(Blade switch, failure): Activate traps **Yes/No** – enterprise-oid : FL MGUARDTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapBladeCtrlPowerStatus (2) – additional : FL MGUARDTrapBladeRackID, FL MGUARDTrapBladeSlotNr, FL MGUARDTrapBladeCtrlPowerStatus This trap is sent when the power supply status of the blade pack changes. – enterprise-oid : FL MGUARDTrapBladeCTRL – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapBladeCtrlRunStatus (3) – additional : FL MGUARDTrapBladeRackID, FL MGUARDTrapBladeSlotNr, FL MGUARDTrapBladeCtrlRunStatus This trap is sent when the blade run status changes.
	Blade reconfiguration	(Backup/restore): Activate traps **Yes/No** – enterprise-oid : FL MGUARDTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapBladeCtrlCfgBackup (1) – additional : FL MGUARDTrapBladeRackID, FL MGUARDTrapBladeSlotNr, FL MGUARDTrapBladeCtrlCfgBackup This trap is sent when configuration backup is triggered for the FL MGUARD BLADE controller.

Management >> SNMP >> Trap (Fortsetzung)		
		– enterprise-oid : FL MGUARDTrapBladeCtrlCfg – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTrapBladeCtrlCfgRestored 2 – additional : FL MGUARDTrapBladeRackID, FL MGUARDTrapBladeSlotNr, FL MGUARDTrapBladeCtrlCfgRestored This trap is sent when configuration restoration is triggered from the FL MGUARD BLADE controller.
CIFS integrity traps	**Successful integrity check of a CIFS share**	Activate traps **Yes/No** – enterprise-oid : FL MGUARDTraPCIC – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTraPCICDone (1) – additional : FL MGUARDTraPCICShareName, FL MGUARDTraPCICShareUNC 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 MGUARDTraPCIC – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTraPCICFail (2) – additional : FL MGUARDTraPCICShareName, FL MGUARDTraPCICShareUNC This trap is sent if the CIFS integrity check has failed.
	Found a (suspicious) difference on a CIFS share	Activate traps **Yes/No** – enterprise-oid : FL MGUARDTraPCIC – generic-trap : enterpriseSpecific – specific-trap : FL MGUARDTraPCICFail (2) – additional : FL MGUARDTraPCICShareName, FL MGUARDTraPCICShareUNC This trap is sent if the CIFS integrity check has detected a deviation.

Management >> SNMP >> Trap (Fortsetzung)		
Userfirewall traps	**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.
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.

Management >> SNMP >> Trap (Fortsetzung)		
		– 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.
	Destination Port	Default: 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.

6.2.6.3 LLDP

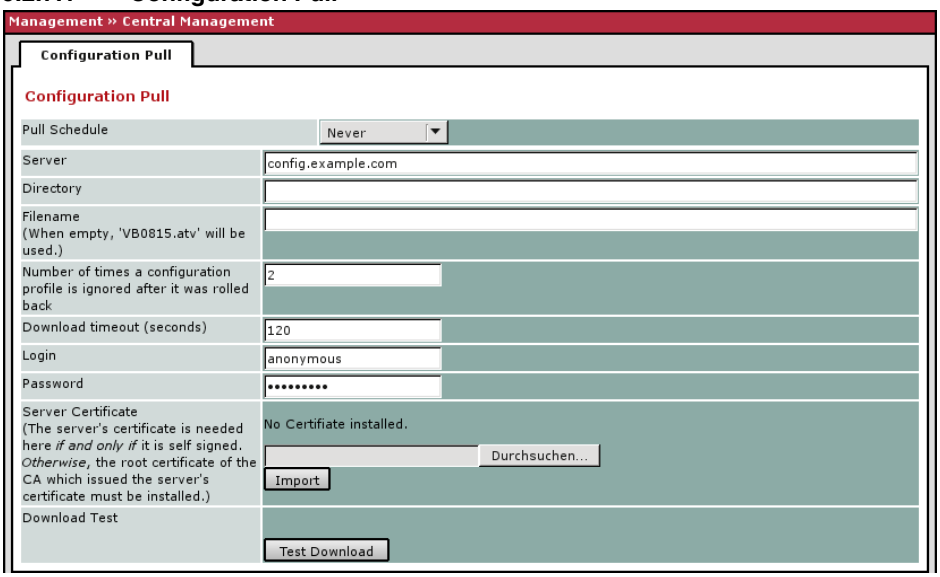


LLDP (Link Layer Discovery Protocol, IEEE 802.1AB/D13) uses suitable request methods to automatically determine the (Ethernet) network infrastructure. LLDP-capable devices periodically send Ethernet multicasts (layer 2). Tables of systems connected to the network are created from the responses, and these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

6.2.7 Management >> Central Management

6.2.7.1 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 FL MGUARD configuration provided differs from the active configuration, the new 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 6-4, “Time and Date” on page 6-7). 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.
	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".

Management >> Central Management >> Configuration Pull (Fortsetzung)

Number of times a configuration profile is ignored after it was rolled back	Default: 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 memorizes the MD5 total for identification purposes, 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 attempts to retrieve a new configuration profile periodically according to the time defined in the **Pull Schedule** field (and **Time Schedule**), 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 and then downloads 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.

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.

Management >> Central Management >> Configuration Pull (Fortsetzung)

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 testing a possibly faulty configuration profile over and over at intervals that are too short. This can block 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 for the FL MGUARD rejection of the new configuration. .

An application note is provided by Innominate. It describes how a rollback can be started using a configuration profile.

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 (Fortsetzung)

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 this individual FL MGUARD using the login and password specified. Otherwise, users of other FL MGUARD devices could access this individual FL MGUARD.

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**.

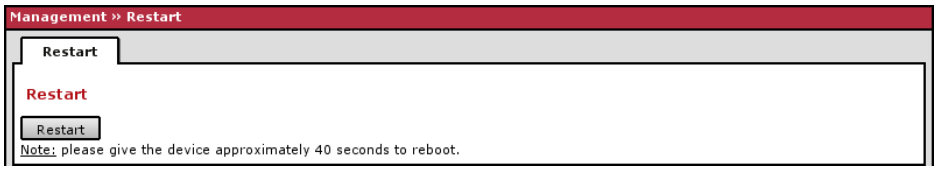
Download Test

- 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.

Ensure that the profile on the server does not contain unwanted variables starting with "GAI_PULL_", as these overwrite the applied configuration.

6.2.8 Management >> Restart

6.2.8.1 Restart



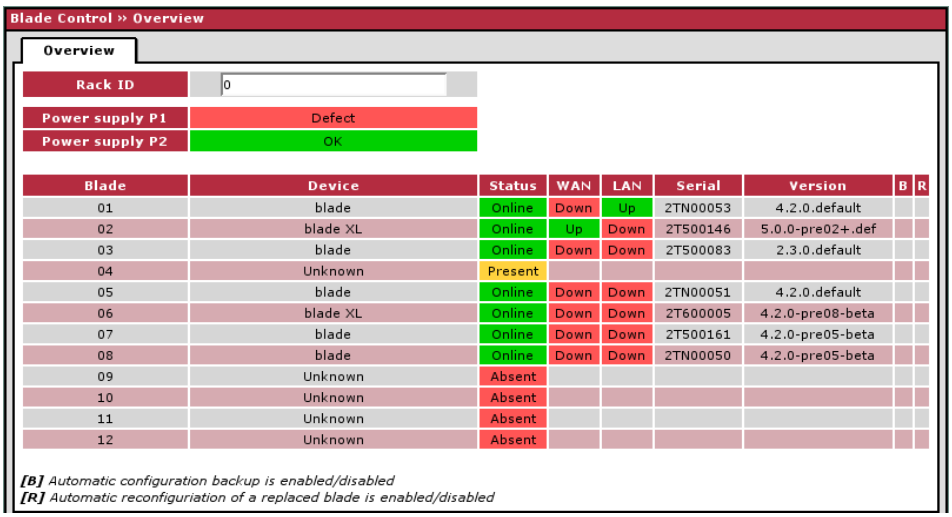
Restarts the FL MGUARD. Has the same effect as a temporary interruption in the power supply, whereby the FL MGUARD is switched off and on again.

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

6.3 Blade Control menu

This menu is only available on the **FL MGUARD BLADE controller**.

6.3.1 Blade Control >> Overview



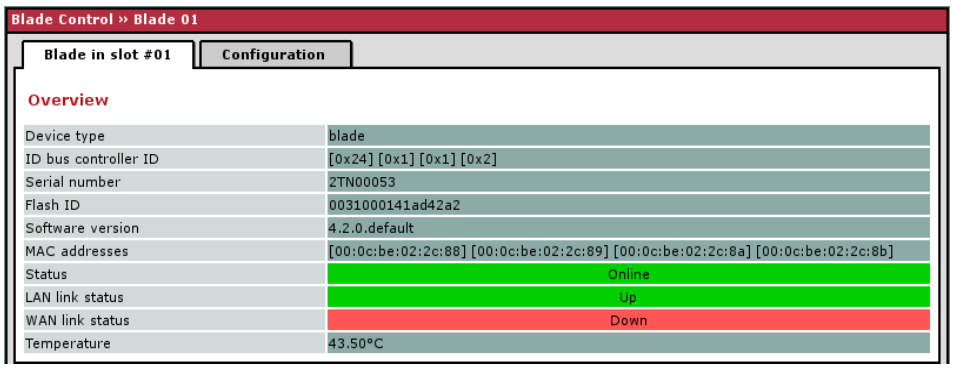
Blade Control >> Overview		
Overview	**Rack ID**	The ID of the rack where the FL MGUARD is located. This value can be configured for all BLADE devices on the controller.
	Power supply P1/P2	Status of power supply units P1 and P2. – OK – Absent – Defect – Fatal error
	Blade	Number of the slot where the FL MGUARD BLADE is installed.
	Device	Device name, e.g., "blade" or "blade XL".
	Status	– **Online -** The device in the slot is operating correctly. – **Present -** The device is present, but not yet ready, e.g., because it is just starting up. – **Absent -** No device found in the slot.
	WAN	Status of the WAN port.
	LAN	Status of the LAN port.
	Serial	Serial number of the FL MGUARD.
	Version	Software version of the FL MGUARD.
	B	**Backup**: Automatic configuration backup on the controller is activated/deactivated for this slot.

Blade Control >> Overview (Fortsetzung)		
	R	**Restore**: Automatic configuration restoration after replacing the FL MGUARD is activated/deactivated for this slot.

6.3.2 Blade Control >> Blade 01 to 12

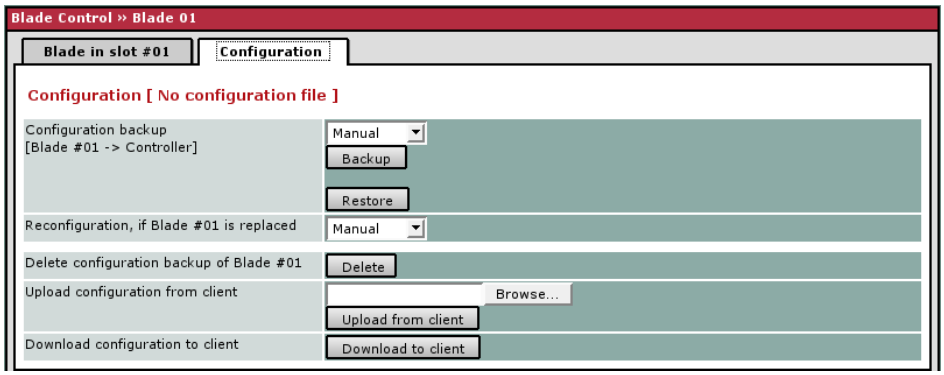
These pages display the status information for each installed FL MGUARD device and enable the configuration of the relevant FL MGUARD device to be backed up and restored.

6.3.2.1 Blade in slot #...



Blade Control >> Blade xx >> Blade in slot xx		
Overview	**Device type**	Device name, e.g., "blade" or "blade XL".
	ID bus controller ID	ID of this slot on the control bus of the BLADEBASE.
	Serial number	Serial number of the FL MGUARD.
	Flash ID	Flash ID of the Flash memory of the FL MGUARD.
	Software version	Version of the software installed on the FL MGUARD.
	MAC addresses	All MAC addresses used by the FL MGUARD.
	Status	Status of the FL MGUARD.
	LAN link status	Status of the LAN port.
	WAN link status	Status of the WAN port.
	Temperature	N/A = Not available

6.3.2.2 Configuration



Blade Control >> Blade xx >> Configuration

Configuration

The status of the stored configuration is displayed for each BLADE:

[No configuration file]

[Obsolete]

[Current]

[File will be copied]

[Blade has been replaced]

[---] No blade available

Configuration backup [Blade #__ -> Controller]

- **Automatic**: The new configuration is stored automatically on the controller shortly after a configuration change on the FL MGUARD.
- **Manual**: The configuration can be stored on the controller by clicking on **Backup**.
- Click on **Restore** to transfer the configuration stored on the controller to the FL MGUARD.

If the blade was reconfigured after a manual configuration backup, but the new configuration was not saved, the configuration stored on the controller is out of date. This is indicated on the *Configuration* tab page by "Configuration [Obsolete]". This indicates that something has been overlooked: in this case, you must backup the configuration on the controller.

Reconfiguration, if the FL MGUARD BLADE is replaced

After replacing an FL MGUARD in this slot, the configuration stored on the controller is automatically transferred to the new device in this slot.

Delete configuration backup of Blade #__

Deletes the configuration stored on the controller for the device in this slot.

Upload configuration from client

Uploads and saves the configuration profile for this slot on the controller.

Download configuration to client

Downloads the configuration profile stored on the controller for this slot onto the configuration PC.

6.4 Network menu

6.4.1 Network >> Interfaces

The FL MGUARD has the following interfaces with external access:

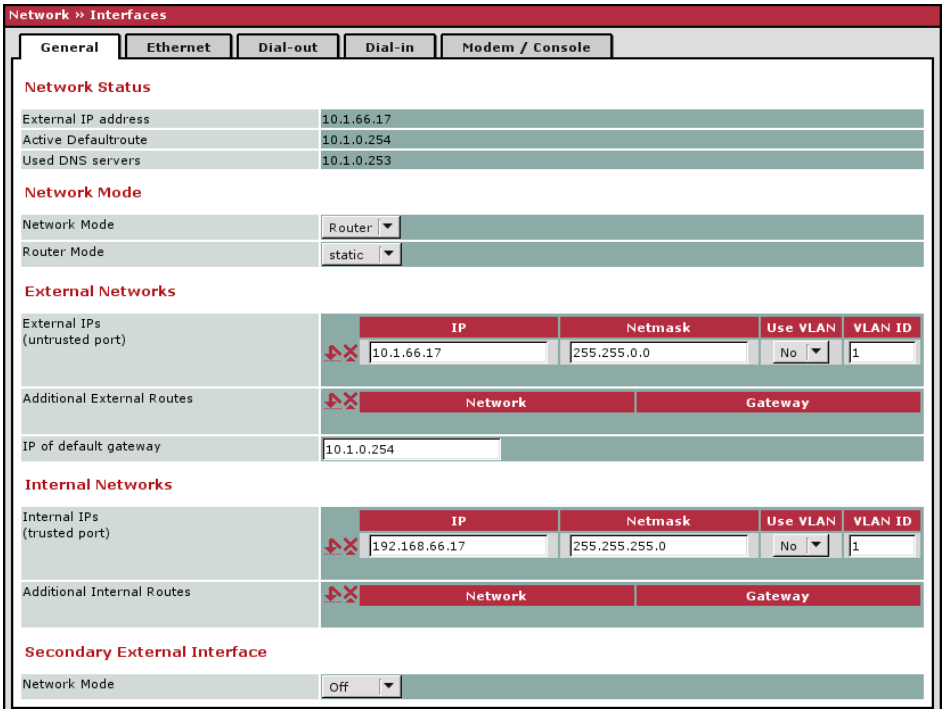
	Ethernet: Internal: LAN External: WAN	Serial interface	Built-in modem	Serial console via USB[1]
FL MGUARD SMART	**Yes**	**No**	**No**	**No**
FL MGUARD SMART2	**Yes**	**No**	**No**	**Yes**
FL MGUARD GT/GT ..., FL MGUARD RS ... , FL MGUARD BLADE, FL MGUARD DELTA	**Yes**	**Yes**	**No**	**No**
Optional: FL MGUARD RS ...	**Yes**	**Yes**	**Yes**	**No**

1 See “Serial console via USB” on page 6-92.

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 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 6-91.

6.4.1.1 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 name 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.

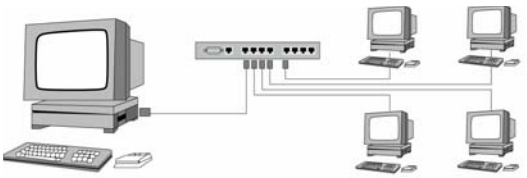
Network >> Interfaces >> General (Fortsetzung)		
Network Mode	**Network Mode**	**Stealth/Router** The FL MGUARD must be set to the network mode that corresponds to its connection to the network (see also “Typical application scenarios” on page 2-1). Depending on which network mode the FL MGUARD is set to, the page will change together with its configuration parameters. See: “Stealth (default settings for FL MGUARD RS ... , FL MGUARD SMART 2, FL MGUARD PCI)” on page 6-60 and “Network Mode: Stealth” on page 6-64 “Router (default settings for FL MGUARD GT/GT ..., FL MGUARD BLADE controller, FL MGUARD DELTA, FL MGUARD RS-B)” on page 6-61 and “Network Mode: Router” on page 6-74
Router Mode	Only used when "Router" is selected as the network mode.	**Static/DHCP/PPPoE/PPTP/Modem[1]/Built-in Modem[1]** See: “Router Mode: static” on page 6-62 and “"Router" network mode, "PPTP" router mode” on page 6-79 “Router Mode: DHCP” on page 6-62 and “"Router" network mode, "DHCP" router mode” on page 6-77 “Router Mode: PPPoE” on page 6-62 and “"Router" network mode, "PPPoE" router mode” on page 6-78 “Router Mode: PPTP” on page 6-62 and “"Router" network mode, "PPTP" router mode” on page 6-79 “Router Mode: Modem” on page 6-63 and “"Router" network mode, "Modem/Built-in Modem" router mode” on page 6-80 “Router Mode: Built-in Modem” on page 6-63 and “"Router" network mode, "Modem/Built-in Modem" router mode” on page 6-80

1 Modem/built-in modem is not available for all FL MGUARD models (see “Network >> Interfaces” on page 6-57).

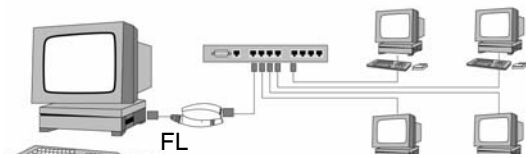
Stealth (default settings for FL MGUARD RS ... , FL MGUARD SMART 2, FL MGUARD PCI)

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:



(A LAN can also be on the left)

The FL MGUARD analyzes the active network traffic and 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.

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).

In *stealth* mode, the FL MGUARD uses internal IP address 1.1.1.1. This can be accessed when the configured default gateway of the computer is also accessible.

In *stealth* network mode, a secondary external interface can also be configured (see “Secondary External Interface” on page 6-68).

For the further configuration of *stealth* network mode, see “Network Mode: Stealth” on page 6-64.

Router (default settings for FL MGUARD GT/GT ..., FL MGUARD BLADE controller, FL MGUARD DELTA, FL MGUARD RS-B)

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 female connector.

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 male connector.
– FL MGUARD PCI:
  In *driver* mode, the LAN port is represented by the network interface of the operating system that has the network card operating system (in this example, FL MGUARD PCI).
  In *power-over-PCI mode*, the LAN port is the LAN female connector of the FLMGUARD PCI.

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

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.

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 6-97).

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 6-68).

There are several router modes, depending on the Internet connection:

– static
– DHCP
– PPPoE
– PPPT
– Modem
– Built-in 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, however, there is 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 peers, is specified by the provider.

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.

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 6-78.

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.)

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.

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 6-97).

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 6-79.

Router Mode: Modem

Only used for *FL MGUARD RS ...* devices *without* a built-in modem, *FL MGUARD BLADE and FL MGUARD DELTA* devices.

If *modem* network mode is selected, the external Ethernet interface of the FL MGUARD is deactivated and data is transferred to and from the WAN via the 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).

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.

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 6-80.

Router Mode: Built-in Modem

Only used for *FL MGUARD RS ...* devices **with** a built-in modem or ISDN terminal adapter.

If *built-in modem* network mode is selected, the external Ethernet interface of the FL MGUARD is deactivated and data is transferred to and from the WAN via the built-in modem or built-in ISDN terminal adapter of the FL MGUARD. This must be connected to the telephone network. The connection to the Internet is then established via the telephone network.

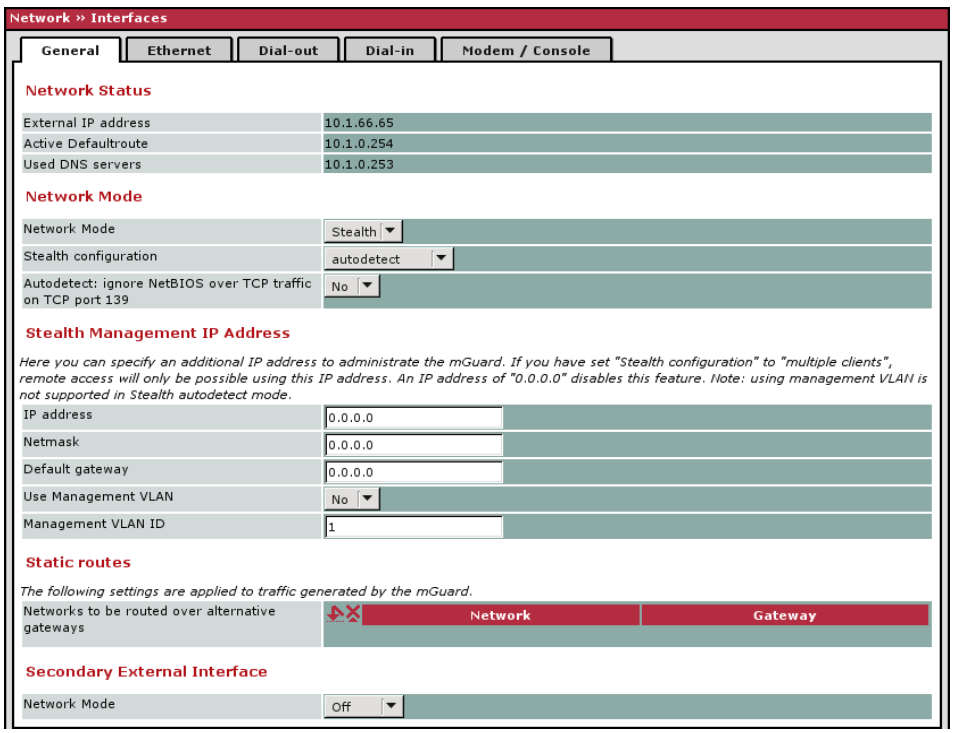
After selecting *built-in modem*, the fields for specifying the modem connection parameters are displayed.

For the further configuration of *built-in modem/modem* network mode, see “"Router" network mode, "Modem/Built-in Modem" router mode” on page 6-80.

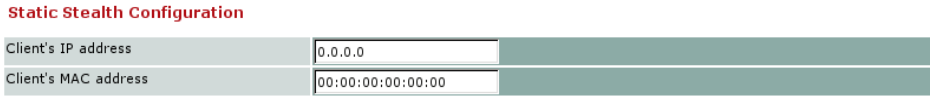
Network Mode: Stealth

Default settings for FL MGUARD RS ... , FL MGUARD SMART 2, FL MGUARD PCI

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



and "static" is selected for the stealth



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

Network Mode

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

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

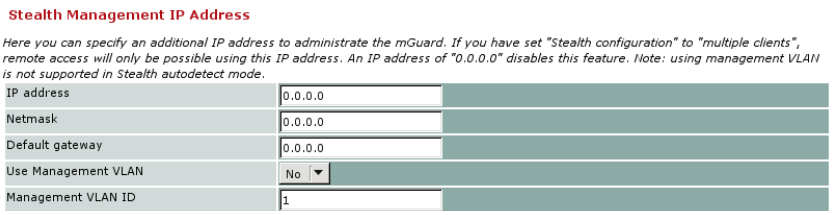
autodetect

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

Network >> Interfaces >> General ("Stealth" network mode) (Fortsetzung)		
		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. **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) (Fortsetzung)

Stealth Management IP Address



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

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

– The **multiple clients** option is selected under *Stealth configuration*
– The client does not answer ARP requests
– No client is available

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.

If the secondary external interface is activated (see “Secondary External Interface” on page 6-68), 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).

IP address — The additional IP address via which the FL MGUARD can be accessed and administered.
The IP address "0.0.0.0" deactivates the management IP address.

Netmask — The subnet mask of the IP address above.

Default gateway — The default gateway of the network where the FL MGUARD is located.

Use Management VLAN: Yes/No — If the IP address should be within a VLAN, set this option to "Yes".

Management VLAN ID — A VLAN ID between 1 and 4095.

VLAN is not supported for the management IP address when *autodetect* stealth configuration is enabled.

For an explanation of this term, please refer to the glossary under “VLAN” on page 8-8.

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

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 in the WAN created by the FL MGUARD. These include the following data traffic packets:

- 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.

Network — Specify the network in CIDR format (see “CIDR (Classless Inter-Domain Routing)” on page 6-220).

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 6-221).

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 to the internal interface (see RFC 2131, Section 4.4.1).

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

Secondary External Interface

Only in *router* network mode **with** *static* router mode or *stealth* network mode. Only for *FL MGUARD RS ...* , *FL MGUARD BLADE, FL MGUARD DELTA*:

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 *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 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, including data traffic generated by the FL MGUARD, can be routed to the external network (WAN) via the secondary external interface.

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 6-91).

Modem/Built-in Modem

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

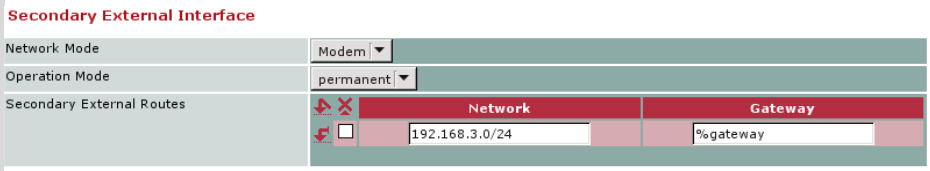
The secondary external interface is created via the serial interface of the FL MGUARD and an external modem connected to it.

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.

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



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 interface activated, and the routing settings for the secondary external interface take effect (see “Probes for Activation” on page 6-71).

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 placeholder.

Operation Mode: permanent/temporary

In both **permanent** and **temporary** 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 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 6-66).
– 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.

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.

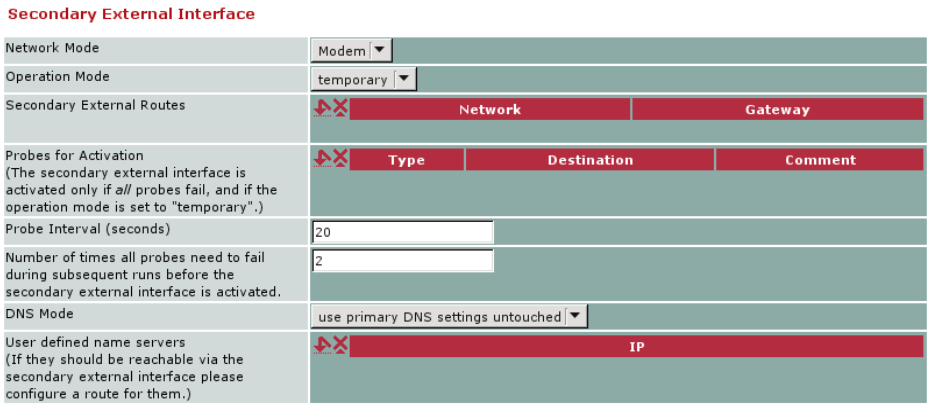
Network >> Interfaces >> General (continued); Secondary External Interface (continued)

Secondary External Interface (continued)

Network Mode = Modem

Operation Mode = temporary

Probes for Activation



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 remote peer 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, so 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 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)

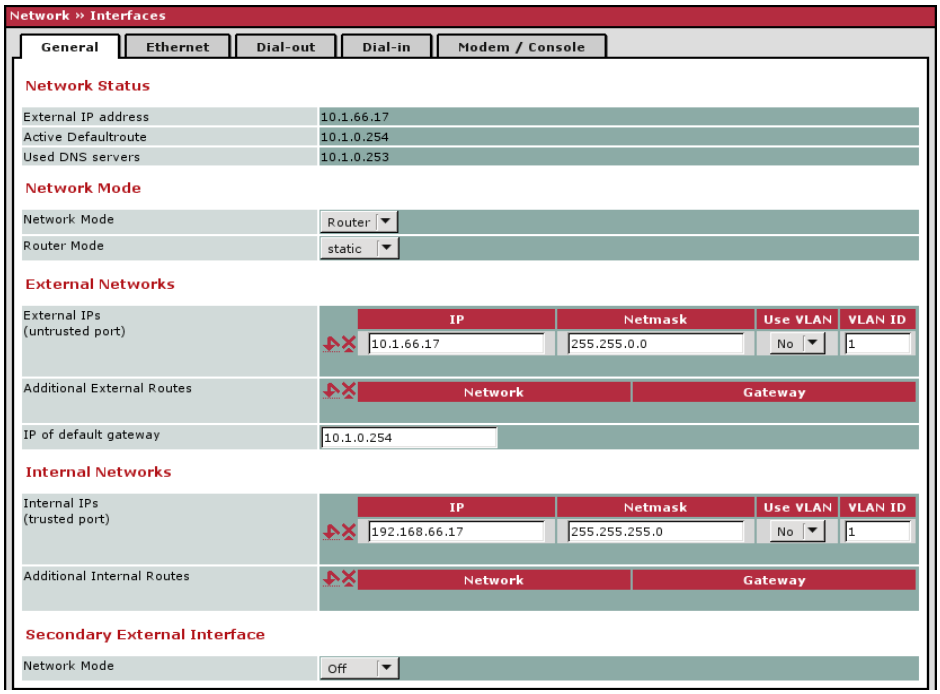
The ping tests defined above under **Probes for Activation...** are performed one after the other. When the ping tests defined are performed once in sequence, this is known as a *test run*. Test runs are performed continuously at intervals. The interval entered in this field specifies how long the FL 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 6-97) 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

Default settings for FL MGUARD GT/GT ..., FL MGUARD DELTA and FL MGUARD BLADE controller

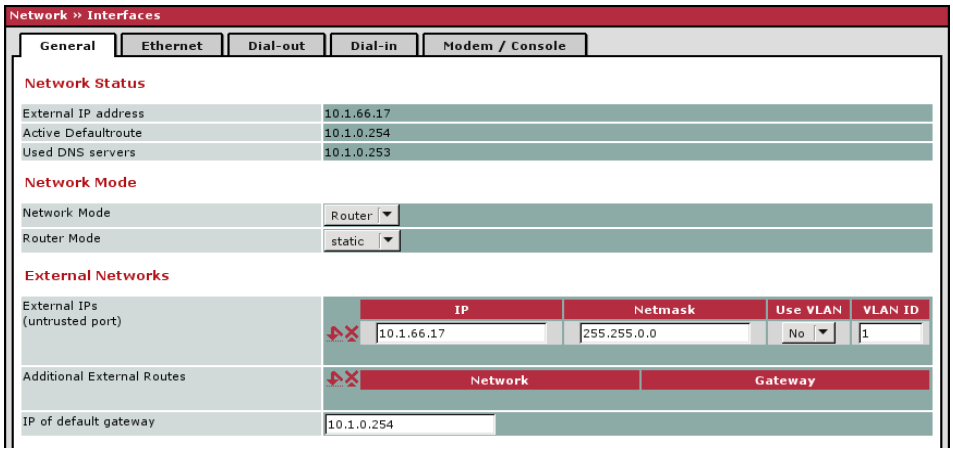
When "Router" is selected as the network mode and "static" is selected as the router mode (see page 6-76)



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**.

Network >> Interfaces >> General ("Router" network mode) (Fortsetzung)		
	VLAN ID	– A VLAN ID between 1 and 4095. – For an explanation of the term "VLAN", please refer to the glossary on page 8-8. – If you want to delete entries from the list, please note that the first entry cannot be deleted.
	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 6-220).
	Gateway	The gateway via which this network can be accessed. See also “Network example diagram” on page 6-221.
Secondary External Interface	See “Secondary External Interface” on page 6-68	

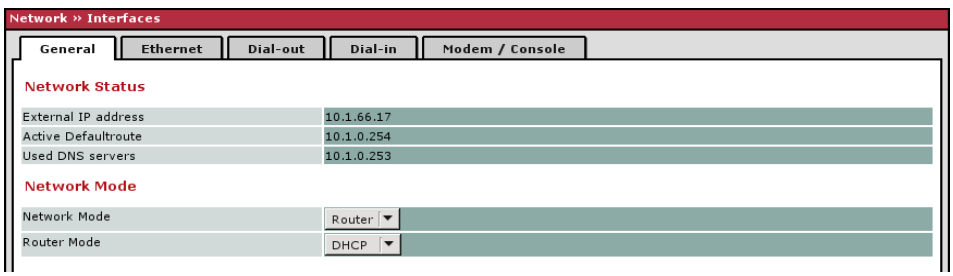
"Router" network mode, "static" router mode



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. – An explanation can be found under “VLAN” on page 8-8. – 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 6-221)

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 6-97).
Internal Networks	See “Internal Networks” on page 6-74.
Secondary External Interface	See “Secondary External Interface” on page 6-68

"Router" network mode, "DHCP" router mode

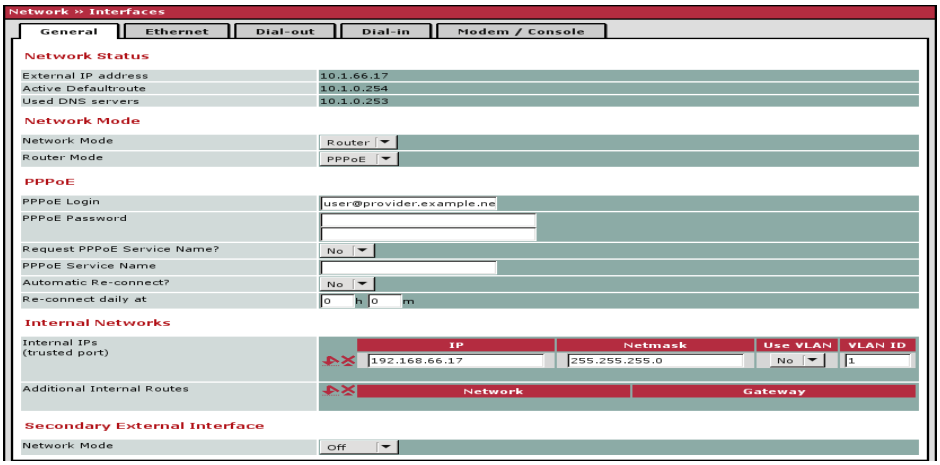


There are no additional setting options for "Router" network mode, "DHCP" router mode.

Network >> Interfaces >> General ("Router" network mode, "DHCP" router mode)	
Internal Networks	See “Internal Networks” on page 6-74.
Secondary External Interface	See “Secondary External Interface” on page 6-68

"Router" network mode, "PPPoE" router mode

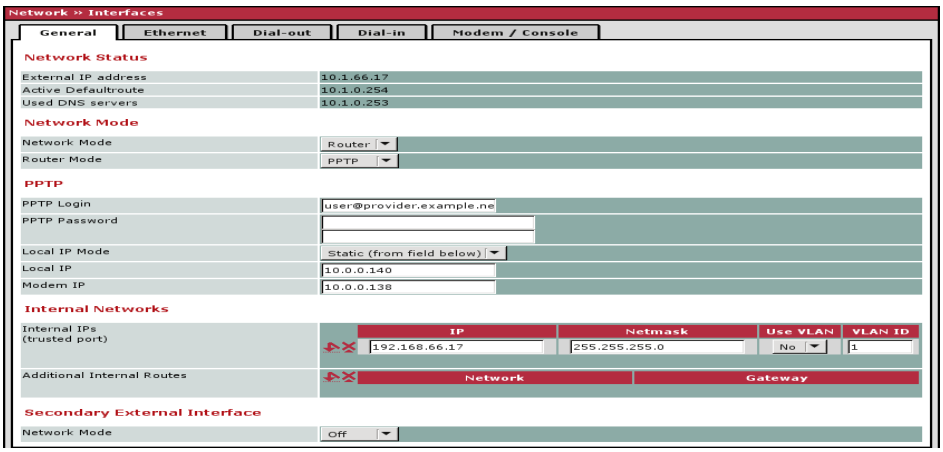
When "Router" is selected as the network mode and "PPPoE" is selected as the router mode



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? — Yes/No 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? — Yes/No 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 6-4, “Time and Date” on page 6-7).
	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 6-74.
Secondary External Interface	See “Secondary External Interface” on page 6-68

"Router" network mode, "PPTP" router mode

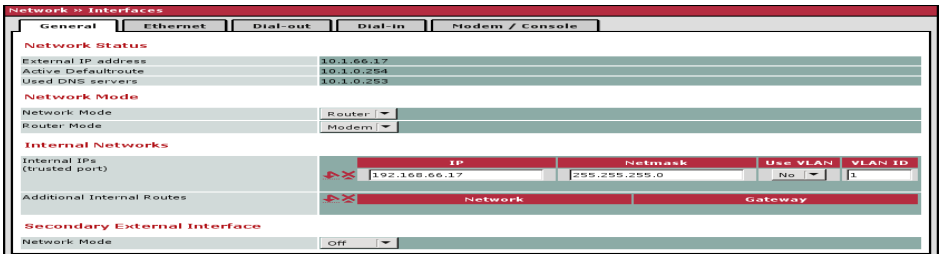
When "Router" is selected as the network mode and "PPTP" is selected as the router mode



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 PPT server of the Internet service provider.
Internal Networks	See “Internal Networks” on page 6-74.
Secondary External Interface	See “Secondary External Interface” on page 6-68

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

Only for *FL MGUARD RS ...*, *FL MGUARD BLADE, FL MGUARD DELTA*



Network >> Interfaces >> General ("Router" network mode, "Modem/Built-in Modem" router mode)

Modem/Built-in Modem

Modem network mode is available for:
FL MGUARD RS ..., FL MGUARD BLADE, FL MGUARD DELTA

Built-in modem network mode is additionally available for:
FL MGUARD RS ..., if it has a built-in modem or a built-in ISDN terminal adapter (optional).

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 either:

- A – Routed via the external serial interface (serial port), to which an external modem must be connected
- B – Routed via the built-in modem/built-in ISDN terminal adapter (for FL MGUARD RS, if equipped accordingly)

In both cases, the connection to the Internet service provider and therefore the Internet is established via the telephone network using a modem or ISDN terminal adapter.

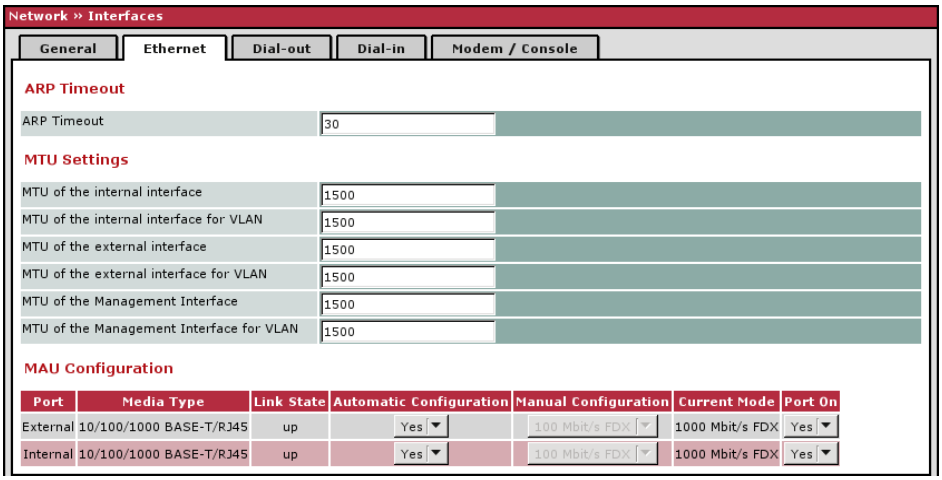
In *modem* network mode, the serial interface of the FL MGUARD is not available for the PPP dial-in option or for configuration purposes (see “Modem/Console” on page 6-91).

After selecting **Modem**[1] 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 6-83 and “Dial-in” on page 6-88).
Enter the connection settings for an external modem on the *Modem/Console* tab page (see “Modem/Console” on page 6-91).

The configuration of the internal networks is described in the next section.

1 **Built-in Modem** can also be selected for the FL MGUARD RS ... (only available as an option for the FL MGUARD RS ... with built-in modem or ISDN terminal adapter).

6.4.1.2 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:

> 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 display 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.

> When connecting the FL MGUARD RS ... to a hub, please note the following: When *Automatic Configuration* is deactivated, the Auto MDIX function is also deactivated. This means that the port of the FL MGUARD RS ... must either be connected to the uplink port of the hub or connected to the hub using a cross-link cable.

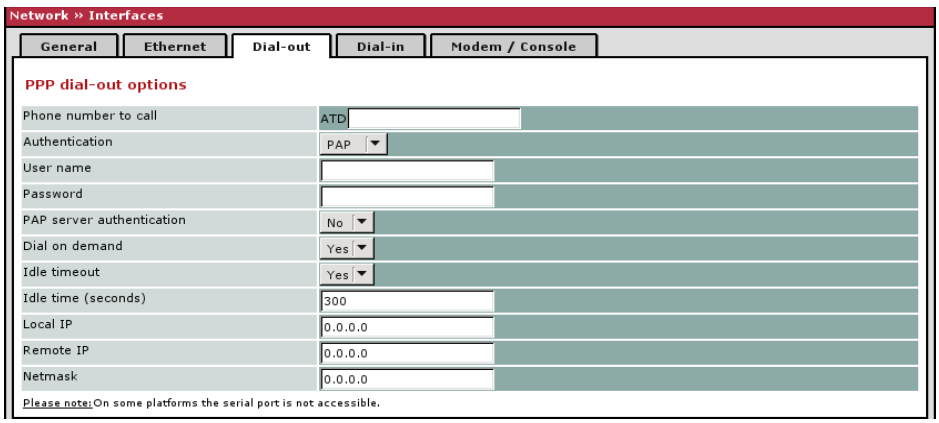
Manual Configuration

The desired operating mode when *Automatic Configuration* is set to *No*.

Network >> Interfaces >> Ethernet		
	Current Mode	The current operating mode of the network connection.
	Port On	**Yes/No** Enables/disables the Ethernet connection. The **Port On** function is supported with restrictions on: – FL MGUARD DELTA: The internal side (switch ports) cannot be switched off – FL MGUARD PCI: In driver mode, the internal network interface cannot be switched off (however, this is possible in power-over-PCI mode)

6.4.1.3 Dial-out

Only for *FL MGUARD RS ..., FL MGUARD BLADE, FL MGUARD DELTA*



Network >> Interfaces >> Dial-out

PPP dial-out options

Should only be configured if the FL MGUARD should 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 modem command for dialing ATD, the following dial sequence is created for the connected modem, for example: 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 (Fortsetzung)	
	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 telephone 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 should be used (only with tone-compatible telephone connections). Example: ATDT765432
Authentication	PAP/CHAP/None PAP = Password Authentication Protocol, CHAP = Challenge Handshake Authentication Protocol. These are 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:	
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:
Server user name **Server password**	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.

Network >> Interfaces >> Dial-out (Fortsetzung)

Subsequent fields

See under “If "None" is selected as the authentication method” on page 6-85.

If authentication is via CHAP:

Local name

A name for the FL MGUARD that it uses to log in to 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 in to 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

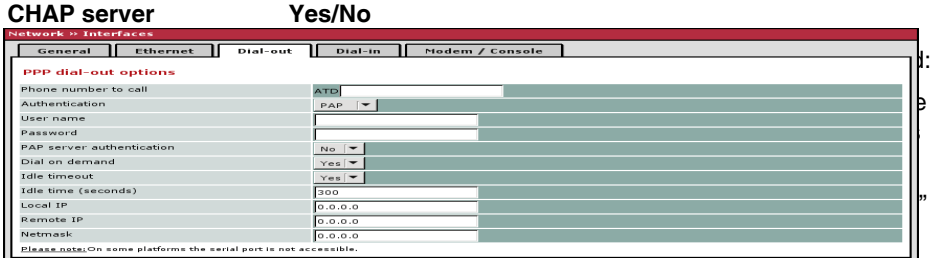
A name assigned to the FL MGUARD by the Internet service provider for identification purposes. The FL MGUARD will not establish a connection to the service provider if the ISP does not assign the correct name.

Secret for client authentication

Password that must be specified during Internet service provider login to access the Internet.

CHAP server

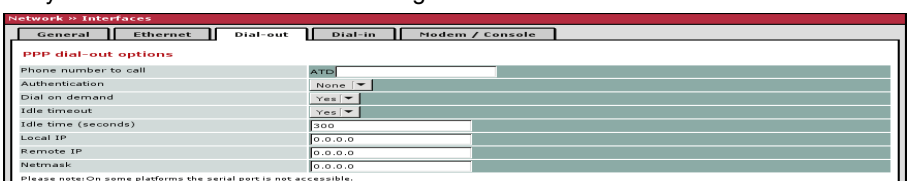
Yes/No



If "None" is selected as the authentication method

In this case all fields that relate to the PAP or CHAP authentication methods are hidden.

Only the fields that define further settings remain visible.



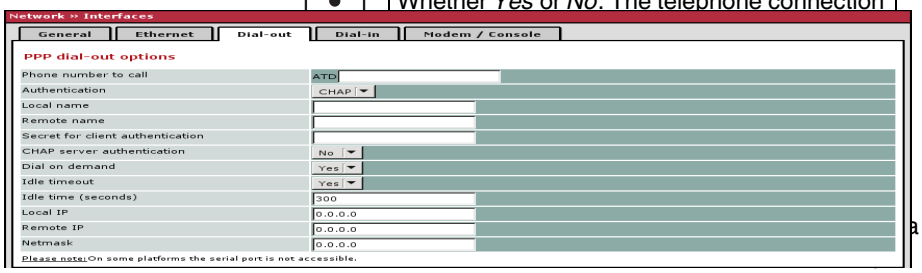
Other common settings

Network >> Interfaces >> Dial-out

PPP dial-out options

Dial on demand Yes/No

Whether *Yes* or *No*: The telephone connection



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 time-out* field). By doing this, the FL MGUARD is not constantly available externally, i.e., for incoming data packets.

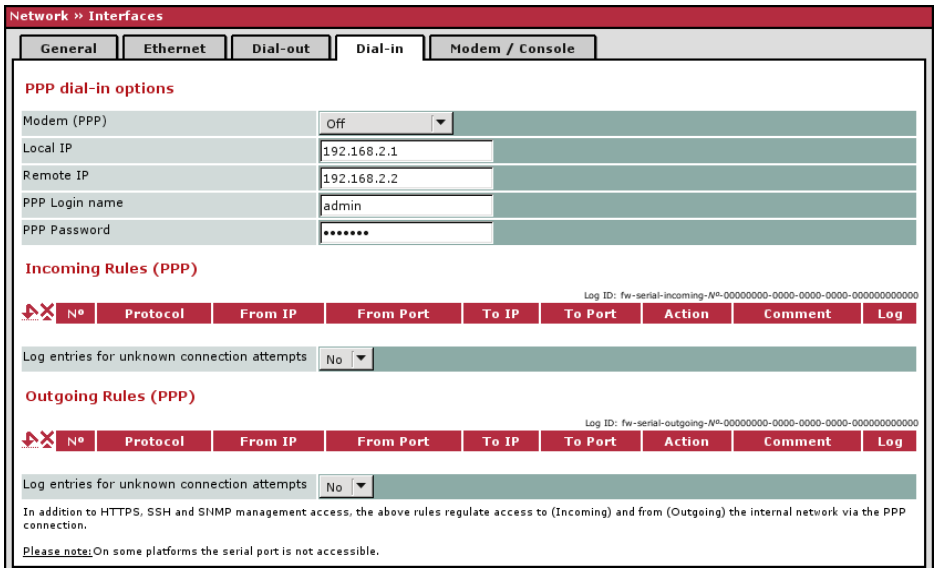
The FL MGUARD also often or sporadically establishes a connection via the modem, or keeps a connection longer, if the following conditions apply:

- 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 remote peer is specified as the host name. After a restart, the FL MGUARD must request the IP address that corresponds to the host name for a DNS server.
- Often: VPN connections are set up and DPD messages are sent regularly (see “Dead Peer Detection” on page 6-192).
- 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 remote peer 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 6-49).

Network >> Interfaces >> Dial-out (Fortsetzung)	
	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 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.
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 remote peer. 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, and 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 6-91).

6.4.1.4 Dial-in

Only for *FL MGUARD RS ...*, *FL MGUARD BLADE, FL MGUARD DELTA*



Network >> Interfaces >> Dial-in

PPP dial-in options

Only for *FL MGUARD RS ...*, *FL MGUARD BLADE, FL MGUARD DELTA*

Should only be configured if the FL MGUARD should permit PPP dial-in via:

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

PPP dial-in can be used to access the LAN (or the FL MGUARD for configuration purposes) (see “Modem/Console” on page 6-91).

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)

Only for *FL MGUARD RS ...* devices (without a built-in modem/ISDN TA), *FL MGUARD BLADE, FL MGUARD DELTA devices*.

Off/On

This option **must** be set to "Off" if no serial interface should 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.

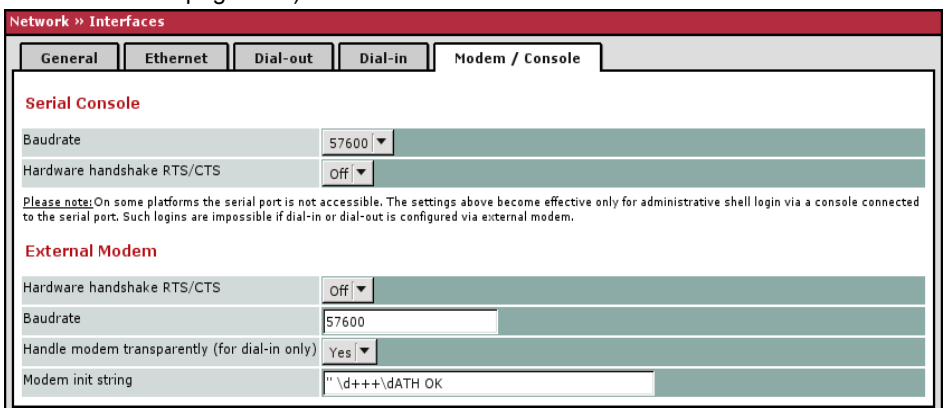
Network >> Interfaces >> Dial-in (Fortsetzung)		
	Modem (PPP)	Only for *FL MGUARD RS ...* (with built-in modem/ISDN TA). **Off/Built-in Modem/External Modem** This option **must** be set to **Off** if no serial interface should be used for the PPP dial-in option. If this option is set to **External Modem**, the PPP dial-in option is available. An external modem must then be connected to the serial interface. The connection settings for the connected external modem should be made on the *Modem/Console* tab page. If this option is set to **Built-in Modem**, the PPP dial-in option is available. In this case, the modem connection is not established via the *serial* female connector on the front. Instead it is established via the terminal strip on the bottom where the built-in modem or ISDN terminal adapter is connected to the telephone network. The connection settings for the built-in modem should be made on the *Modem/Console* tab page. If the **Built-in Modem** option is used, the serial interface can also be used. For the options for using the serial interface, see “Modem/Console” on page 6-91.
	Local IP	IP address of the FL MGUARD via which it can be accessed for a PPP connection.
	Remote IP	IP address of the remote peer of the PPP connection.
	PPP Login name	Login name that must be specified by the PPP remote peer in order to access the FL MGUARD via a PPP connection.
	PPP Password	The password that must be specified by the PPP remote peer 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, 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 6-220)
	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).

Network >> Interfaces >> Dial-in (Fortsetzung)		
	Action	**Accept** means that the data packets may pass through. **Reject** means that the data packets are sent back, so the sender is informed of their rejection. **Drop** means that the data packets may not 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)
	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 connection initiated by PPP dial-in.

6.4.1.5 Modem/Console

Only for *FL MGUARD RS ...*, *FL MGUARD BLADE, FL MGUARD DELTA, FL MGUARD SMART2 (not for FL MGUARD SMART)*

Some FL MGUARD models have a serial interface that can be accessed externally, while the FL MGUARD RS ... is also available with a built-in modem as an option (see “Network >> Interfaces” on page 6-57).



Options for using the serial interface

Alternatively, the serial interface can be used as follows:

Primary External Interface

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 6-57 and “General” on page 6-58).
In this case, data traffic is not processed via the WAN port (Ethernet interface), but via the serial interface.

Secondary External Interface

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 6-57 and “General” on page 6-58).
In this case data traffic is processed (permanently or temporarily) via the serial interface.

For dialing in to the LAN or for configuration purposes

Used for **dialing in to the LAN or for configuration purposes** (see also “Dial-in” on page 6-88). 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.

  On 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

The following settings for the *baud rate* and *hardware handshake* are only valid for a configuration connection where a terminal or PC with terminal program is connected to the serial interface.

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 (Only for FL MGUARD SMART 2, does not apply to FL MGUARD SMART)	**No/Yes** When **No** is selected, the FL MGUARD SMART 2 uses the USB connection solely as a power supply When **Yes** is selected, the FL MGUARD SMART 2 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 SMART 2 provides a console through the serial interface, which can then be used in the terminal program. A driver is required when using Windows. It can be downloaded at www.innominate.de.

External Modem

Hardware handshake RTS/CTS	**Off/On** When set to **On**, flow is controlled by means of RTS and CTS signals for PPP connections.
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.

Network >> Interfaces >> Modem/Console

Handle modem transparently (for dial-in only)	**Yes/No** If the external modem is used for dial-in (see page 6-88), **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 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 manual for the initialization sequence.

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 specify that 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**.

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 without changing the modem default settings.

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.

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.

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.

For the FL MGUARD RS ... with built-in modem/built-in ISDN modem (ISDN terminal adapter)

The FL MGUARD RS ... is available with a built-in analog modem/built-in ISDN terminal adapter as an option. The built-in modem or built-in ISDN terminal adapter can be used as follows:

Primary External Interface

– As a **primary external interface**, if the network mode is set to *Built-in Modem* under *Network* >> *Interfaces* on the *General* tab page (see “Network >> Interfaces” on page 6-57 and “General” on page 6-58). In this case, data traffic is not processed via the WAN port (Ethernet interface), but via this modem.

Secondary External Interface

– As a **secondary external interface**, if *Secondary External Interface* is activated and *Built-in Modem* is selected under *Network* >> *Interfaces* on the *General* tab page (see “Network >> Interfaces” on page 6-57 and “General” on page 6-58). In this case data traffic is also processed via the serial interface.

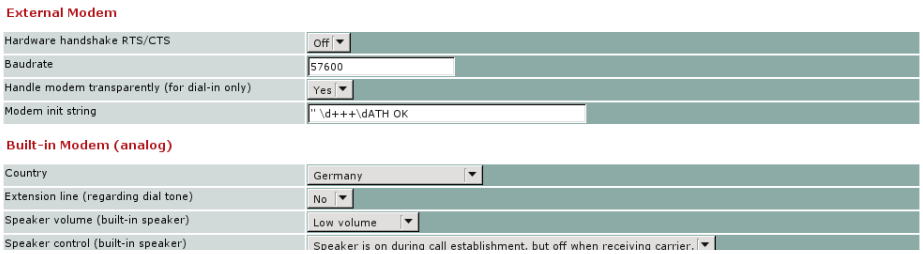
PPP dial-in options

– For the PPP dial-in option (see “Options for using the serial interface” on page 6-91).

Please note that the serial interface of the device also provides similar options for use (see above). Therefore on an *FL MGUARD RS ...* with a built-in modem, normal data traffic can be routed via a modem connection (*modem* network mode) and a second modem connection can be used simultaneously for the PPP dial-in option, for example.

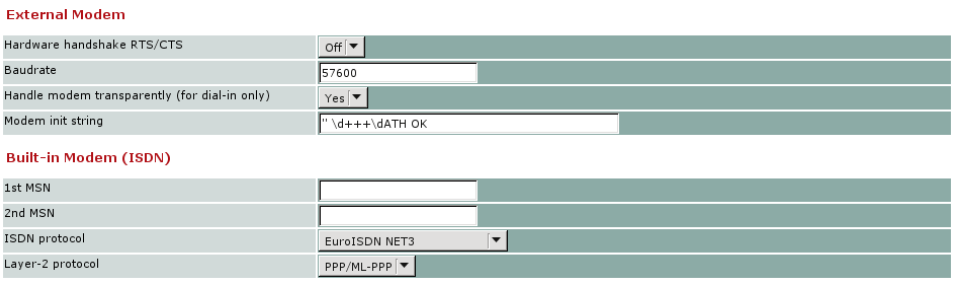
For the FL MGUARD RS ... with built-in modem

Additionally for the FLMGUARD RS ... with built-in modem (analog)



Network >> Interfaces >> Modem/Console (for the FL MGUARD RS ... with built-in modem)		
External Modem	**As for the *FL MGUARD RS ...* (without built-in modem), *FL MGUARD BLADE*, and *FL MGUARD DELTA*:** Configuration as above for **External Modem** (see “External Modem” on page 6-92).	
Built-in Modem (analog)	**Country**	The country where the FL MGUARD with built-in modem is operated must be specified here. This ensures that the built-in modem operates according to the applicable remote access guidelines in the respective country and that it recognizes and uses dial tones correctly, for example.
	Extension line (regarding dial tone)	Yes/No When set to **No**, the FL MGUARD waits for the dial tone when the telephone network is accessed and the FL MGUARD is calling the remote peer. When set to **Yes**, the FL MGUARD does not wait for a dial tone. Instead it begins dialing the remote peer immediately. This procedure may be necessary if the built-in modem of the FL MGUARD is connected to a private branch exchange that does not emit a dial tone when it is "picked up". When a specific number must be dialed to access an external line, e.g., "0", this number should be added to the start of the desired remote peer phone number that is to be dialed.
	Speaker volume (built-in speaker)	
	Speaker control (built-in speaker)	These two settings specify which sounds should be emitted by the FL MGUARD speaker and at what volume.

For the FL MGUARD RS ... with built-in ISDN terminal adapter

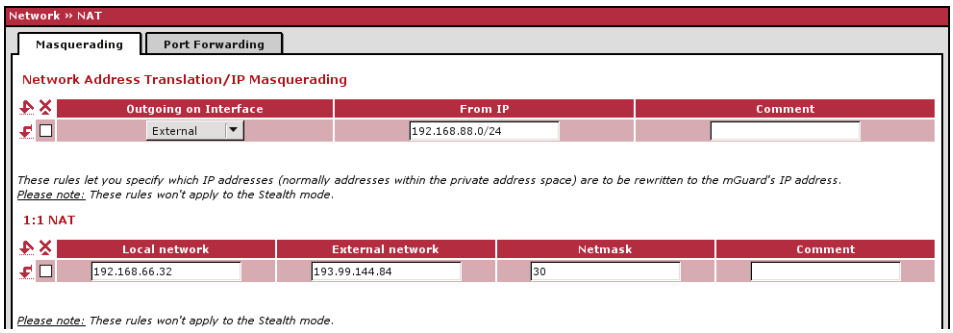


Additionally for the FL MGUARD RS ... with built-in modem (ISDN)

Network >> Interfaces >> Modem/Console (for the FL MGUARD RS ... with built-in ISDN terminal adapter)		
External Modem	**As for the *FL MGUARD RS ...* (without built-in modem), *FL MGUARD BLADE*, and *FL MGUARD DELTA*:** Configuration as above for **External Modem** (see “External Modem” on page 6-92).	
Built-in Modem (ISDN)	**1st MSN**	For outgoing calls, the FL MGUARD transmits the MSN (Multiple Subscriber Number) entered here to the called remote peer. In addition, the FL MGUARD can receive incoming calls via this MSN (provided dial-in operation is enabled – see *General* tab page). Maximum of 25 alphanumeric characters; the following special characters can be used: *****, **#**, **:** (colon)
	2nd MSN	If the FL MGUARD should also receive incoming calls via another number for dial-in operation (if enabled), enter the second MSN here.
	ISDN protocol	The EuroISDN protocol (also known as NET3) is used in Germany and many other European countries. Otherwise the ISDN protocol should be specified according to the country. If necessary, this must be requested from the relevant phone company.
	Layer-2 protocol	The set of rules used by the ISDN terminal adapter of the local FL MGUARD to communicate with its ISDN remote peer. This generally is the ISDN modem of the Internet service provider used to establish the connection to the Internet. It must be requested from the Internet service provider. PPP/ML-PPP is often used.

6.4.2 Network >> NAT

6.4.2.1 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.

Network >> NAT >> Masquerading (Fortsetzung)

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.

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)).

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 6-133).

Please observe the incoming rules when using the "Internal" setting (see “Incoming Rules” on page 6-131).

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 6-220)

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.

192.168.0.0/24 **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 (Fortsetzung)

Default settings: 1:1 NAT is not active.

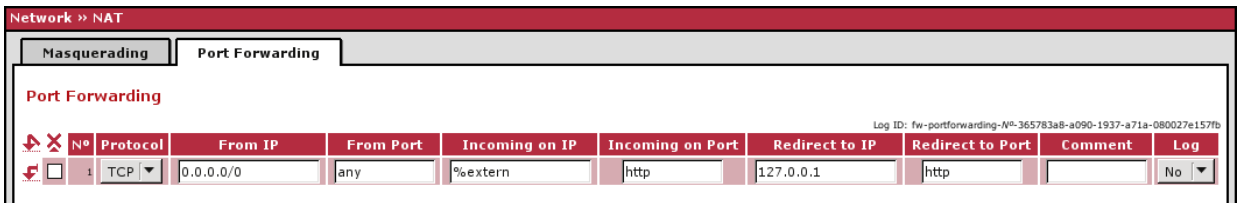
1:1 NAT cannot be applied to the e*xternal 2* interface.

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 6-220).
Comment	Can be filled with appropriate comments.

[1] *External 2* and *All External* are only for devices with a serial interface: FL MGUARD RS ..., FL MGUARD BLADE, FL MGUARD DELTA (see “Secondary External Interface” on page 6-68).

6.4.2.2 Port Forwarding



Network >> NAT >> Port Forwarding

Port Forwarding

Lists the rules defined for port forwarding (DNAT = Destination NAT).

Port forwarding includes the following: The header 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, i.e., the IP address and port number in the header of incoming data packets are changed.

This method is also referred to as Destination NAT.

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

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

Protocol: TCP/UDP — Specify the protocol to which the rule should apply.

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 6-220)

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.

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.

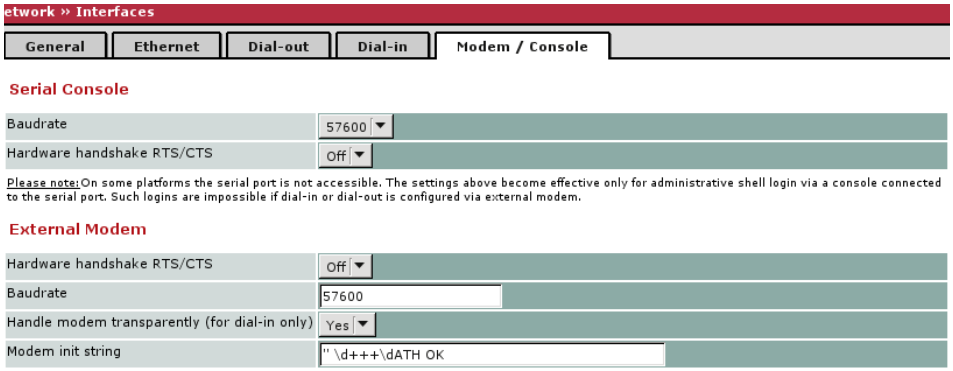
Incoming on Port — The original destination port specified in the incoming data packets.

Either the port number or the corresponding service name can be specified here, e.g., *pop3* for port 110 or *http* for port 80.

Network >> NAT >> Port Forwarding (Fortsetzung)		
	Redirect to IP	The internal IP address to which the data packets should be forwarded. The original destination addresses will be overwritten with this address.
	Redirect to Port	The port to which the data packets should be forwarded. The original destination port will be overwritten with this 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.
	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)

6.4.3 Network >> DNS

6.4.3.1 DNS server



Network >> DNS >> DNS server

DNS

If the FL MGUARD is to initiate a connection to a remote peer 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 (Fortsetzung)

Local Resolving of Hostnames

You can configure multiple entries with assignment pairs of host names and IP addresses for various domain names.

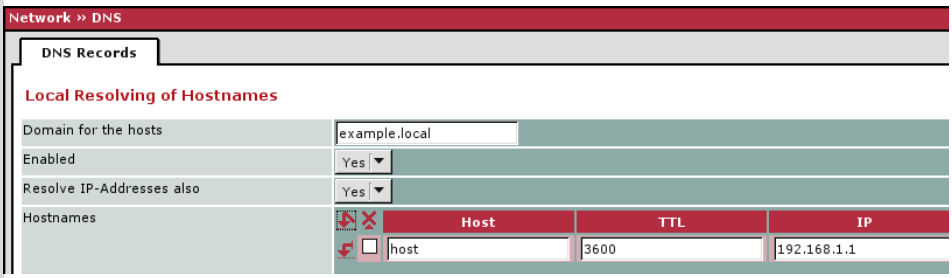
You have the option to define, change (edit), and delete assignment pairs of host names and IP addresses. You can also activate or deactivate the resolving of host names for a domain. In addition, you can delete a domain with all its assignment pairs.

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* functions 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 to host names.

Yes: Same as for "No". However, it is also possible to get the host name assigned to an IP address.

Hostnames
The table can have any number of entries.

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 his notebook on site to connect to the local network for machine A, B or C and to communicate with the individual control systems. In order for the technician not to have to know and enter the IP address for every single control system in machine A, B or C, host names are assigned to the IP addresses of the control systems 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 control system 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 his notebook to the local network at machine A, B or C and use the same host name in each of these networks to communicate with the corresponding machine control systems.

The notebook can obtain the IP address to be used, the name server, and the domain from the FL MGUARD via DHCP.

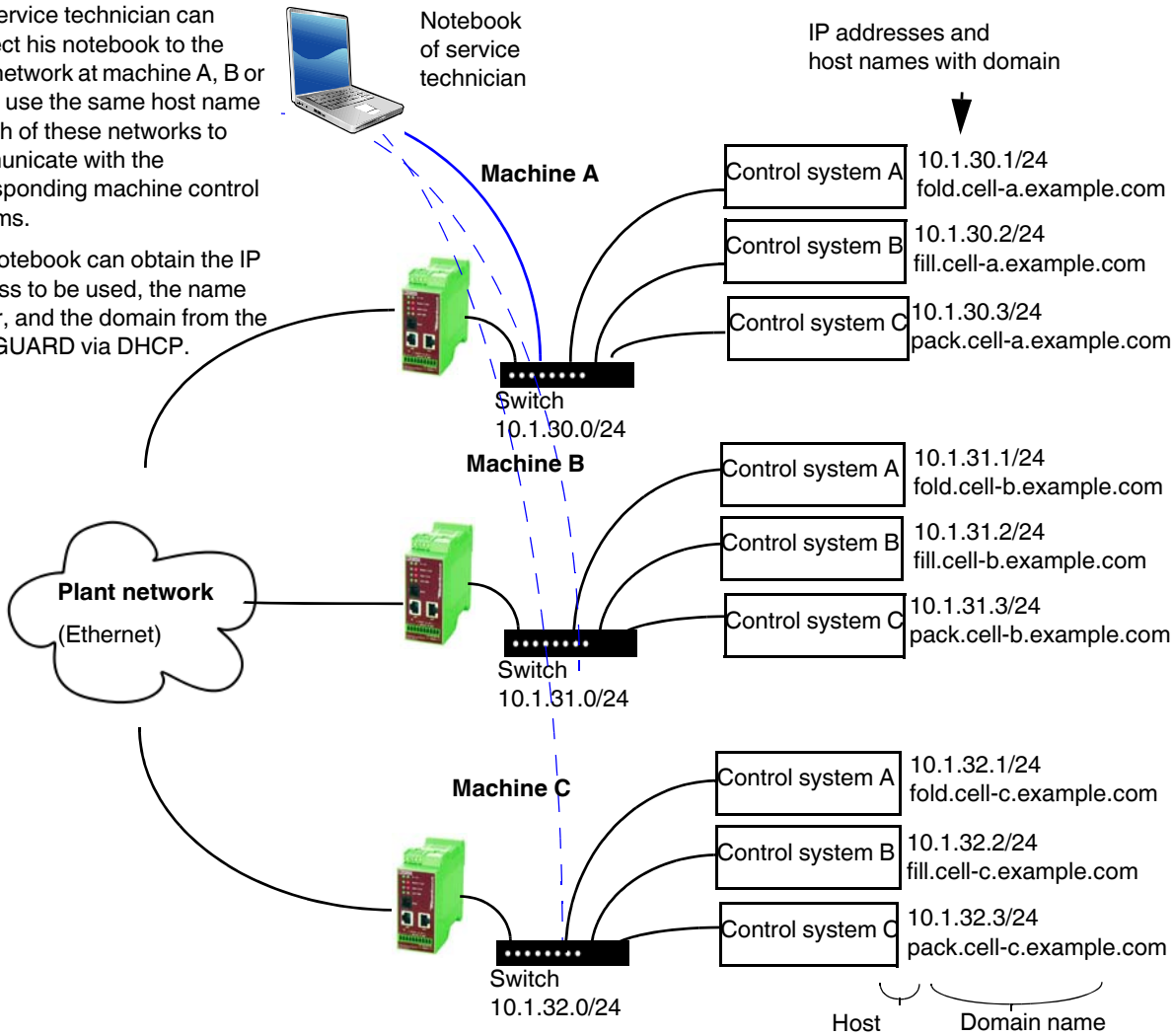
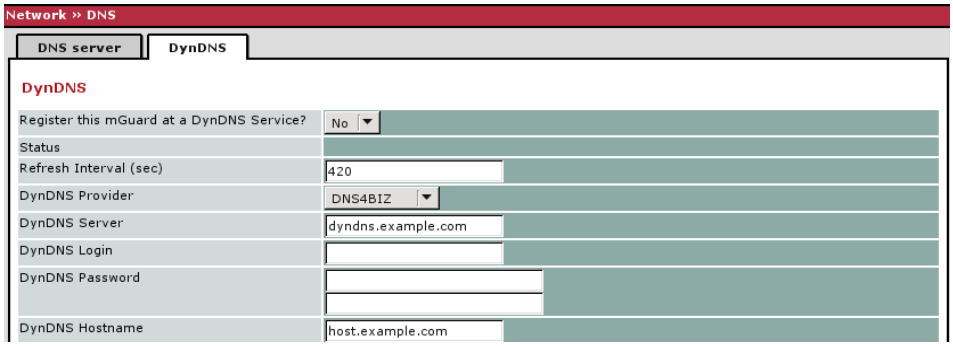


Figure 6-1 Local resolving of host names

6.4.3.2 DynDNS



Network >> DNS >> DynDNS

DynDNS

At least one partner IP address must be known in order to establish a VPN connection so that they 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 the 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 the FL MGUARD should use this service. The FL MGUARD then reports its current IP address to the DynDNS service (i.e., the one assigned for Internet access 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 be accessed via this host name.

6.4.4 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).

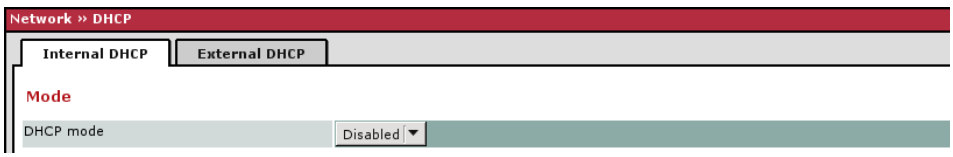
The DHCP server also operates in *stealth* mode.

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.

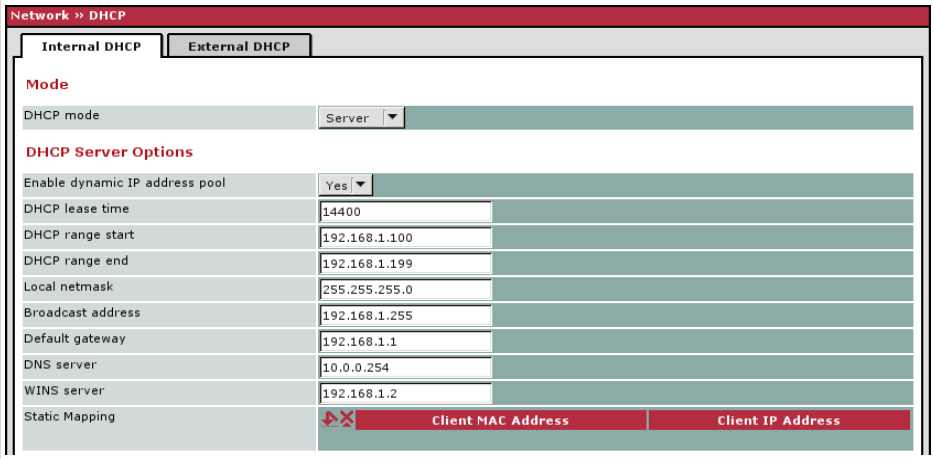
6.4.4.1 Internal/External DHCP



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"). 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.
	DHCP mode	**Server**

Network >> DHCP >> Internal DHCP (Fortsetzung)

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 elapses. 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 computers to release host names in IP addresses via the Domain Name Service (DNS).

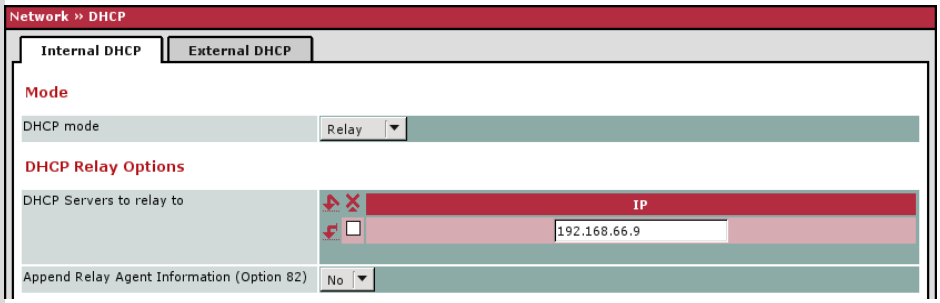
If the DNS service of the FL MGUARD should be used, enter the internal IP address of the FL MGUARD here.

Network >> DHCP >> Internal DHCP (Fortsetzung)	
WINS server	Address of the server used by the computer to release 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) – Client's IP address **Client IP Address** The static IP address of the computer to be assigned to the MAC address. Static assignments take priority over the dynamic IP address pool. Static assignments must not overlap with the dynamic IP address pool. Do not use one IP address in multiple static assignments, otherwise multiple MAC addresses will be assigned to this IP address. Only one DHCP server should be used per subnetwork.

Network >> DHCP >> Internal DHCP (Fortsetzung)

DHCP mode **Relay**

If DHCP mode is set to *Relay*, the corresponding setting options are displayed below as follows.



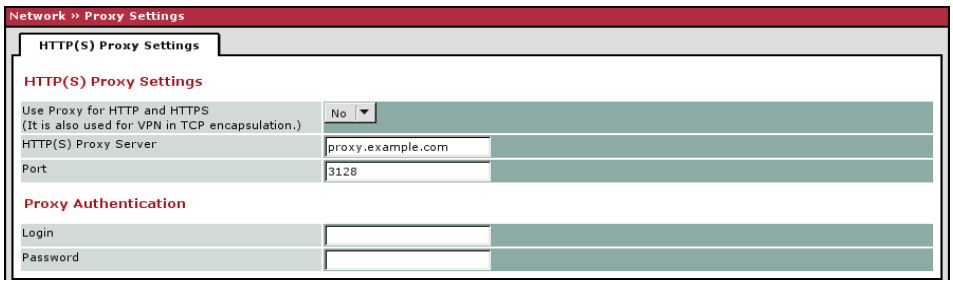
DHCP Relay Options

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 that are being forwarded to can be appended according to RFC 3046.

6.4.5 Network >> Proxy Settings

6.4.5.1 HTTP(S) Proxy Settings



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

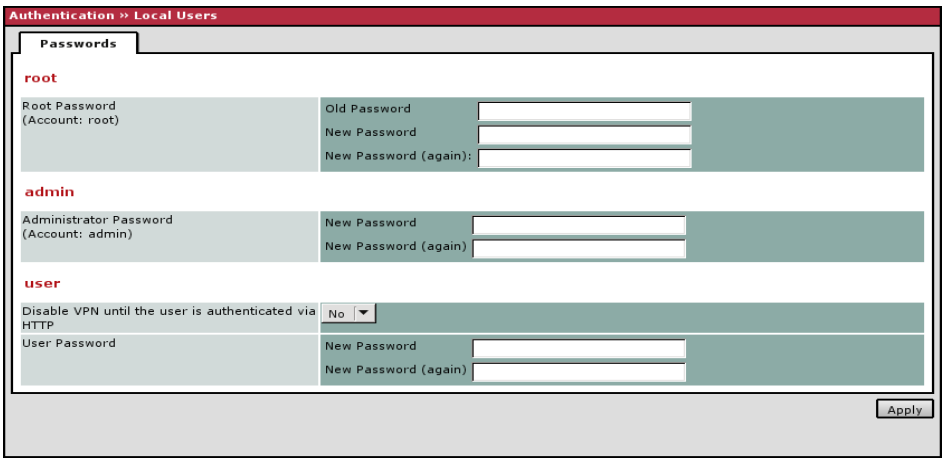
– CRL download
– Firmware update
– Regular configuration profile retrieval from a central location
– Restoring of licenses

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.

6.5 Authentication menu

6.5.1 Authentication >> Local Users

6.5.1.1 Passwords



Local 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 >> Local 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**

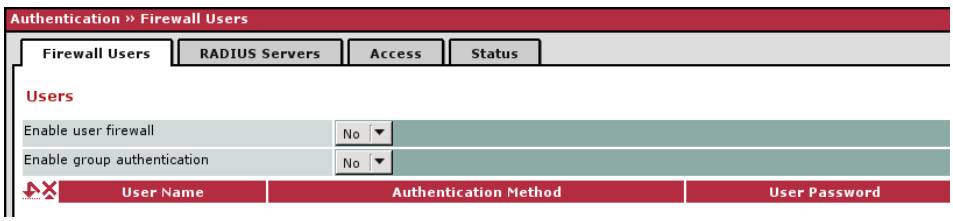
Authentication >> Local Users >> Passwords (Fortsetzung)		
user	**Disable VPN until the user is authenticated via HTTP**	If a user password has been specified and activated, the user must always enter this password after an FL MGUARD restart **in order to enable FL MGUARD VPN connections** when attempting 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.

6.5.2 Authentication >> Firewall Users

For example, to prevent private surfing on the Internet, every outgoing connection is blocked under *Network Security* >> *Packet Filter* >> *Sets of Rules* . VPN is not affected by this.

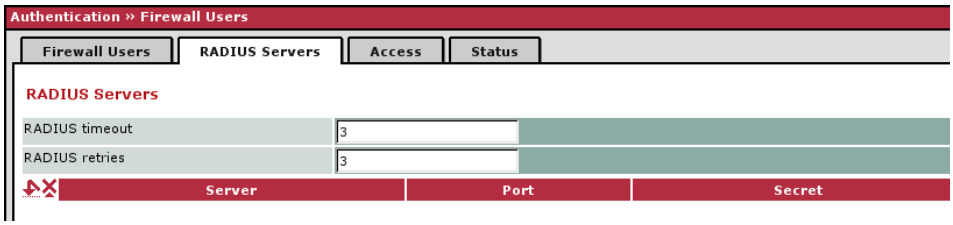
Under *Network Security* >> *User Firewall* , different firewall rules can be defined for certain users, e.g., outgoing connections are permitted. This user firewall rule takes effect as soon as the relevant firewall user (to whom this user firewall rule applies) has logged in, see “Network Security >> User Firewall” on page 6-144.

6.5.2.1 Firewall Users



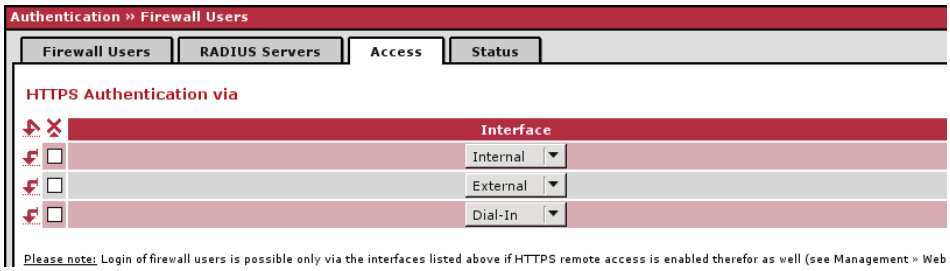
Authentication >> Firewall Users >> Firewall Users		
Users	**Lists the firewall users by their assigned user names. Also specifies the authentication method.**	
	Enable user firewall	Under the *Network Security* >> *User Firewall* menu item, firewall rules can be defined and assigned to specific firewall 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" package as a "Filter-ID=<group-name>" attribute.
	User Name	Name the user must enter on 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.

6.5.2.2 RADIUS Servers



Authentication >> Firewall Users >> RADIUS Servers		
RADIUS Servers	**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
	Server	Name of the RADIUS server or its IP address.
	Port	The port number used by the RADIUS server.
	Secret	RADIUS server password.

6.5.2.3 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 6-145.

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 6-21).

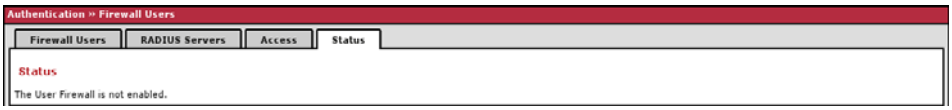
In *stealth* network mode, both the **internal** and **external** interfaces must be enabled so that firewall users can log in to the FL MGUARD.

(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 6-57).

6.5.2.4 Status

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



6.5.3 Authentication >> Certificates

Authentication is a fundamental element of secure communication. Using certificates, the X.509 authentication method ensures that the "correct" partners communicate with each other. 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 6-170, “Authentication” on page 6-183).
– Management of the FL MGUARD via SSH (shell access) (see “Management >> System Settings” on page 6-4, “Shell Access” on page 6-11).
– Management of the FL MGUARD via HTTPS (see “Management >> Web Settings” on page 6-20, “Access” on page 6-21).

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 remote peers (e.g., for an operator attempting to access the FL MGUARD remotely via HTTPS and a web browser). A certificate specific to an individual can be saved on a chip card and then inserted in the card reader of the relevant computer when prompted by a web browser, 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 their remote peer (partner B), partner B then shows their certificate to their remote peer (partner A).

In order for A to accept the certificate shown by B, i.e., the certificate of the remote peer, (thus allowing communication), there is the following option: A has previously received a copy of the certificate from B (e.g., by data carrier or e-mail), with which B will verify itself. A can then verify the certificate shown later by B by comparing it to this certificate. 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 remote peer in order to use X.509 authentication for communication at a later time. The PKCS#12 file contains a private key that must be kept secret and must not be given to a third party (see “Creation of certificates” on page 6-117).

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 6-123).

CA certificates

The certificate shown by a remote peer 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 remote peers in accordance with X.509, the method described below of consulting CA certificates can be used instead or as an additional measure.

CA certificates provide a way of checking whether the certificate shown by the remote peer is really signed by the CA specified in the remote peer'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 remote peer is authentic using the CA certificates loaded on the FL MGUARD. This requires that all CA certificates must be available to the FL MGUARD in order to form a chain with the certificate shown by the remote peer. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the remote peer 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 remote peers to be extended without any increased management effort, as the installation of a remote certificate for each possible remote peer is not compulsory.

Creation of certificates

To create a certificate, a *private key* and the corresponding *public key* are required. Programs are available which can be used to create these keys. 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 principle methods of X.509 authentication.

– The authentication of a remote peer 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 remote peer is authentic. This requires that all CA certificates must be available to the FL MGUARD in order to form a chain with the certificate shown by the remote peer through to the root certificate.

"Available" means that the corresponding CA certificates must be installed on the FL MGUARD (see “CA certificates” on page 6-125) and must also be referenced during the configuration of the corresponding application (SSH, HTTPS, and VPN).

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

Authentication for SSH

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

1 (See “Management >> System Settings” on page 6-4, “Shell Access” on page 6-11)

Authentication for HTTPS

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

1 The remote peer 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 6-20, “Access” on page 6-21)

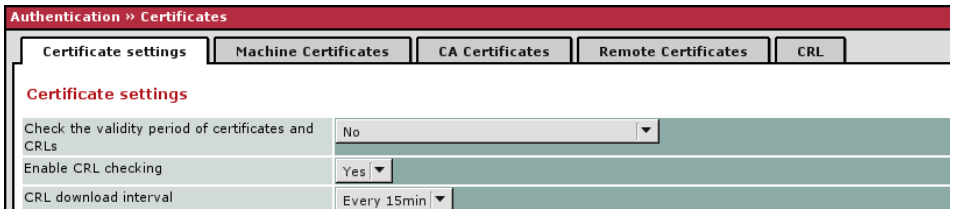
Authentication for VPN

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

6.5.3.1 Certificate settings



Authentication >> Certificates >> Certificate settings

Certificate settings

The settings made here relate to the certificates and certificate chains that are to be checked by the FL MGUARD.

This generally excludes the following:

– Self-signed certificates from remote peers
– All remote certificates for VPN

Check the validity period of certificates and CRLs: No/Wait for synchronization of the system time

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 RS ...*, FL MGUARD GT/GT ..., *FL MGUARD DELTA* and for the *FL MGUARD SMART2* but not for the *FL MGUARD SMART*), or
– By synchronizing the system clock (see “Time and Date” on page 6-7)

Until this point, all certificates to be checked are considered invalid.

Authentication >> Certificates >> Certificate settings (Fortsetzung)

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 6-129), 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 6-129), 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.

6.5.3.2 Machine certificates

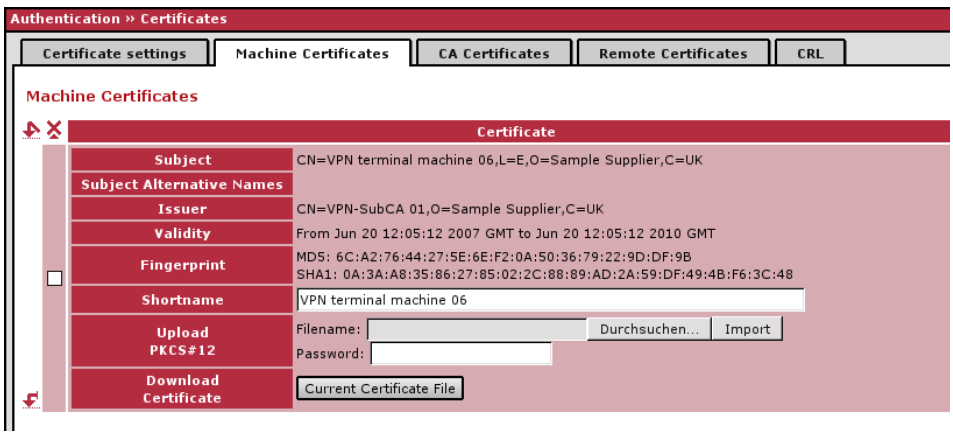
The FL MGUARD authenticates itself to the remote peer using a machine certificate loaded on the FL MGUARD. The machine certificate acts as an ID card for the FL MGUARD, which it shows to the relevant remote peer.

For a more detailed explanation, see “Authentication >> Certificates” on page 6-116.

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 a CA-signed machine certificate to the remote peer for various connections.

In order to use the installed machine certificate 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 for 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 remote peers, 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.

Shortname

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 remote peer in order to authenticate the FL MGUARD). This copy does not contain the private key and can be made public at any time.

To do this, proceed as follows:

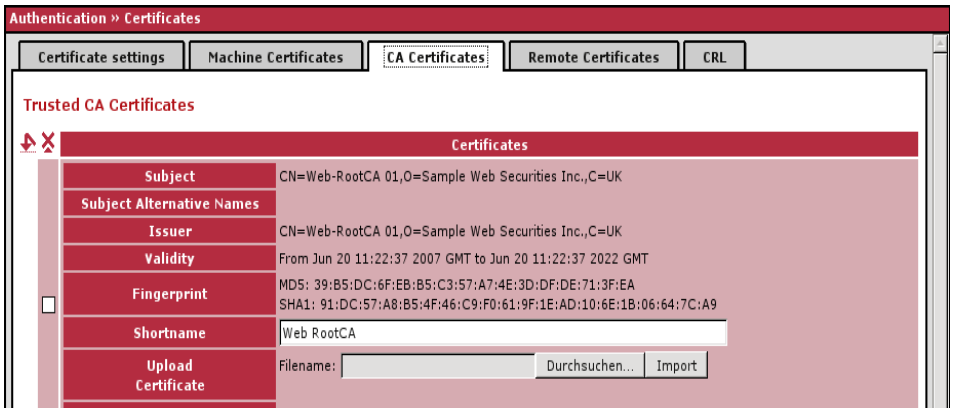
- Click on **Current Certificate File** next to the *Download Certificate* row for the relevant machine certificate.
- Enter the desired information in the dialog box that opens.

6.5.3.3 CA certificates

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

The checking process is as follows: The certificate issuer (CA) is specified as the issuer in the certificate shown by the remote peer. These details can be verified by the same issuer using the local CA certificate. For a more detailed explanation, see “Authentication >> Certificates” on page 6-116.

Example for imported CA certificates:



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.

Shortname

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.

6.5.3.4 Remote certificates

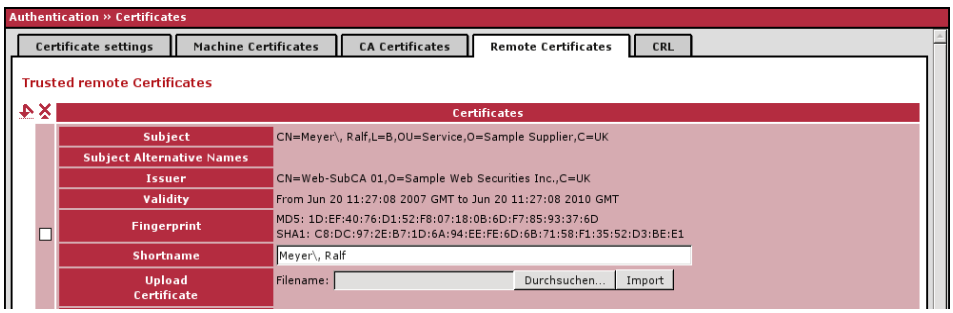
A remote certificate is a copy of the certificate that is used by a remote peer to authenticate itself to the FL MGUARD.

Remote certificates are files (file name extension: *.cer, *.pem or *.crt) received from possible remote peers by trustworthy means. Load these files on the FL MGUARD so that reciprocal authentication can take place. The remote certificates of several possible remote peers 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 6-116.

Example for 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.

Shortname

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.

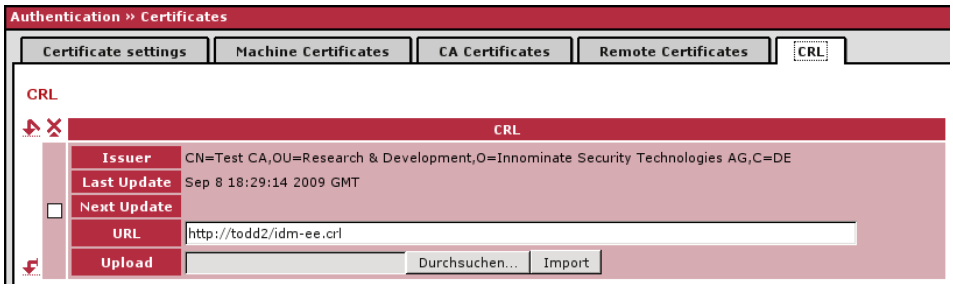
Creating a certificate copy

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.

6.5.3.5 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 where 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 6-121).

A CRL with the same issuer name must be present for each issuer name specified in the certificate 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 6-121).

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.

6.6 Network Security menu

This menu is **not** available on the **FL MGUARD BLADE** controller.

6.6.1 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.

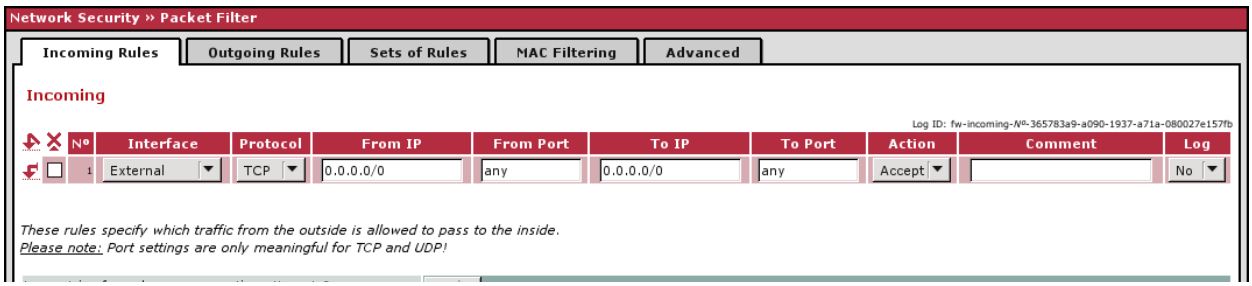
The firewall rules here have an effect on the firewall that is permanently active, with the exception of:

– **VPN connections**. Individual firewall rules are defined for VPN connections (see “IPsec VPN >> Connections” on page 6-170, “Firewall” on page 6-189).
– **User firewall**. When a user logs on, for whom user firewall rules are defined, these rules take priority (see “Network Security >> User Firewall” on page 6-144), followed by the permanently active firewall rules.

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.

6.6.1.1 Incoming Rules



Network Security >> Packet Filter >> Incoming Rules

Incoming

Lists the firewall rules that have been set up. They apply for incoming data connections that have been initiated externally.

If no rule has been set, the data packets of all incoming connections (excluding VPN) are dropped (default settings).

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, 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 6-220).

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, so the sender is informed of their rejection. .

> In stealth mode, **Reject** has the same effect as **Drop**.

Drop means that the data packets may not 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 *Sets of Rules* tab page).

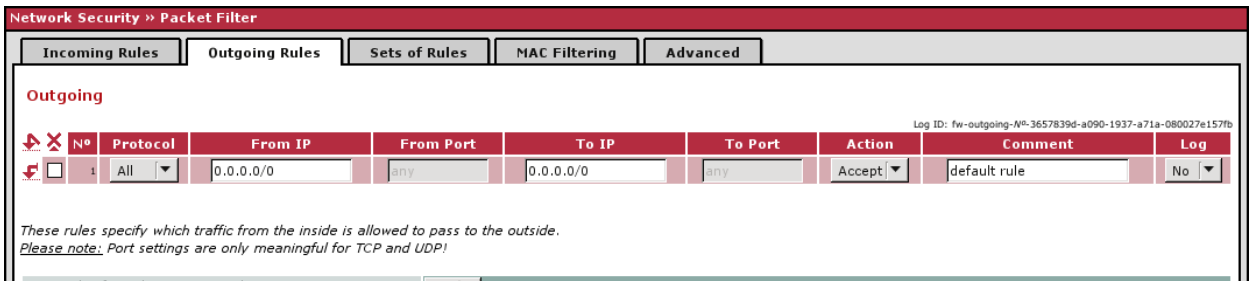
Comment

Freely selectable comment for this rule.

Network Security >> Packet Filter >> Incoming Rules (Fortsetzung)		
	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 6-57).

6.6.1.2 Outgoing Rules



Network Security >> Packet Filter >> Outgoing Rules

Outgoing

Lists the firewall rules that have been set up. They apply for outgoing data connections that have been initiated internally in order to communicate with a remote partner.

Default settings: A rule is defined by default that allows all outgoing connections.

If no rule is defined, all outgoing connections are prohibited (excluding VPN).

Protocol — TCP, UDP, ICMP, 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 6-220).

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, so the sender is informed of their rejection. .

> In stealth mode, **Reject** has the same effect as **Drop**.

Drop means that the data packets may not 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 *Sets of Rules* tab page).

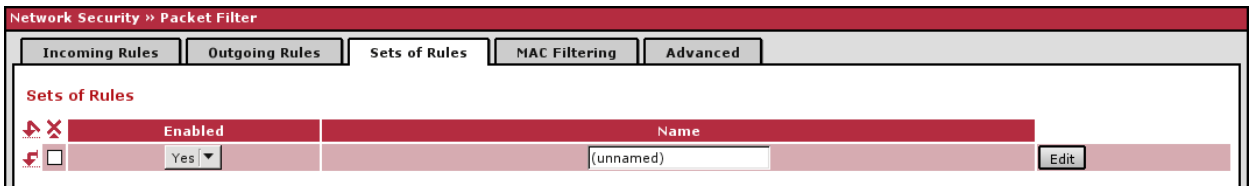
Comment — Freely selectable comment for this rule.

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)

Network Security >> Packet Filter >> Outgoing Rules (Fortsetzung)		
	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**)

6.6.1.3 Sets of Rules



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 comprises 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 >> Sets of Rules

Sets of Rules

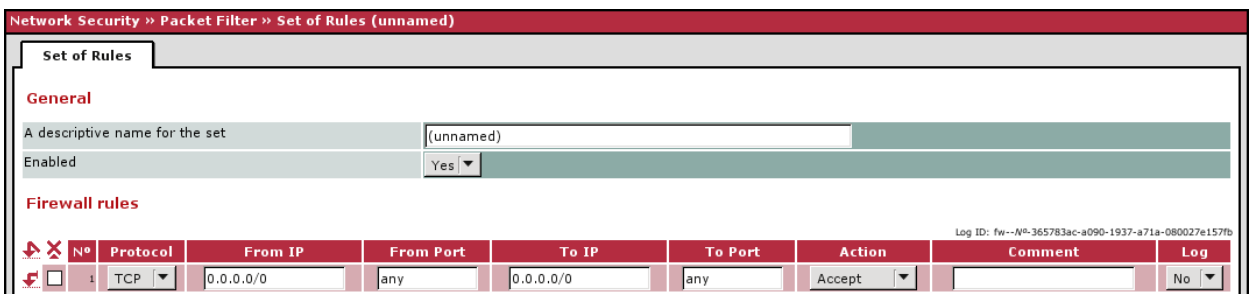
Lists all the defined firewall sets of rules.

Sets of rules are only used if they are referenced on the *Incoming Rules* or *Outgoing Rules* tab page.

A set or 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 or rules. The name is specified when the set or rules is created.

The **Set of Rules** page is displayed when you click on *Edit*:

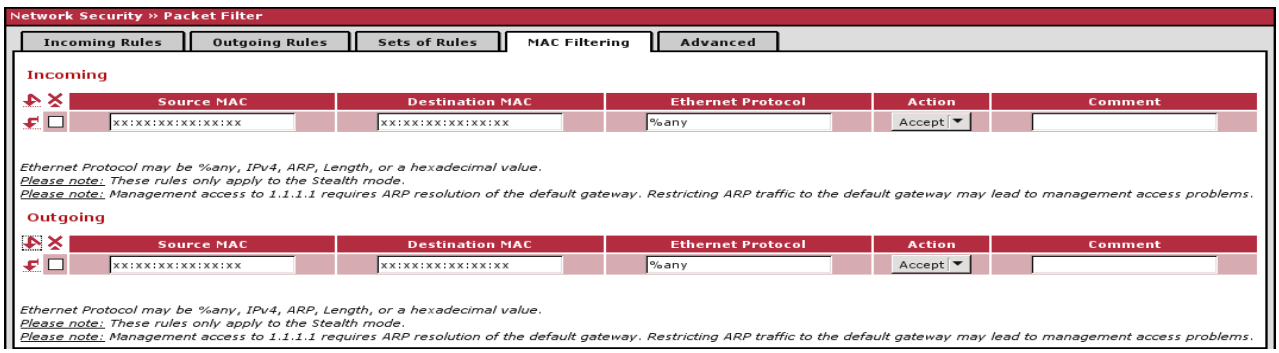


General

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.

Network Security >> Packet Filter >> Sets of Rules (Fortsetzung)		
	Enabled	Activates/deactivates the relevant set of rules.
Firewall rules	**Protocol**	TCP, UDP, ICMP, 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 6-220).
	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, so the sender is informed of their rejection. In stealth mode, **Reject** has the same effect as **Drop**. **Drop** means that the data packets may not 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)

6.6.1.4 MAC Filtering



The MAC filter is only applied to data packets that are received or sent via the Ethernet 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 (Layer2) 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 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.

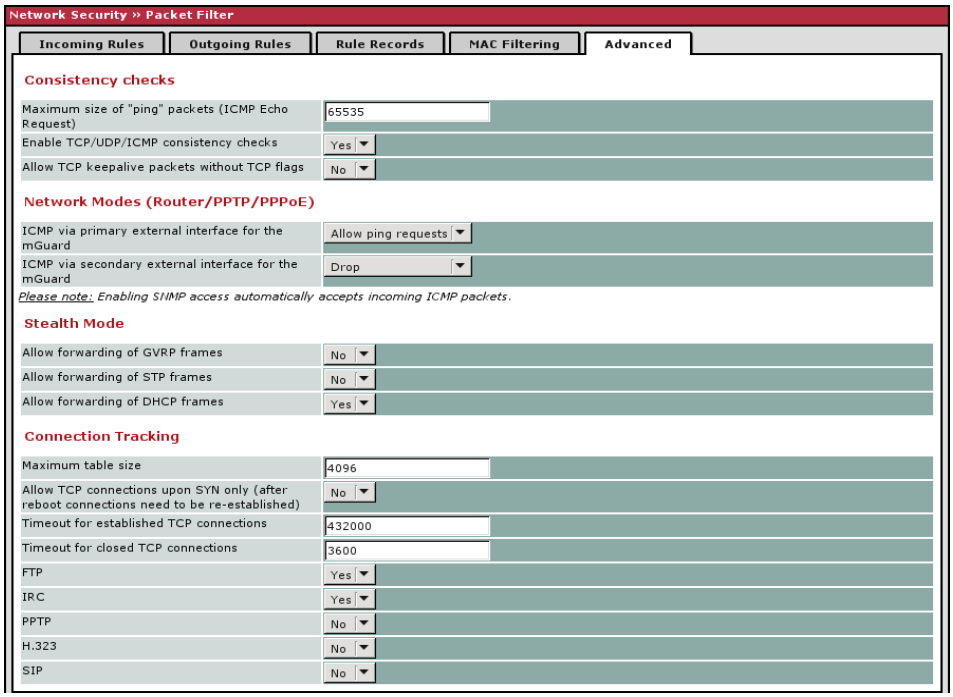
The MAC filter does not support logging.

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 are sent, for example.
	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 may not pass through (they are dropped).
	Comment	Freely selectable comment for this rule.

1 FL MGUARD RS ..., FL MGUARD BLADE, FL MGUARD DELTA

6.6.1.5 Advanced

The following settings affect the basic behavior of the firewall.



Network Security >> Packet Filter >> Advanced		
Consistency checks	**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 should 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.

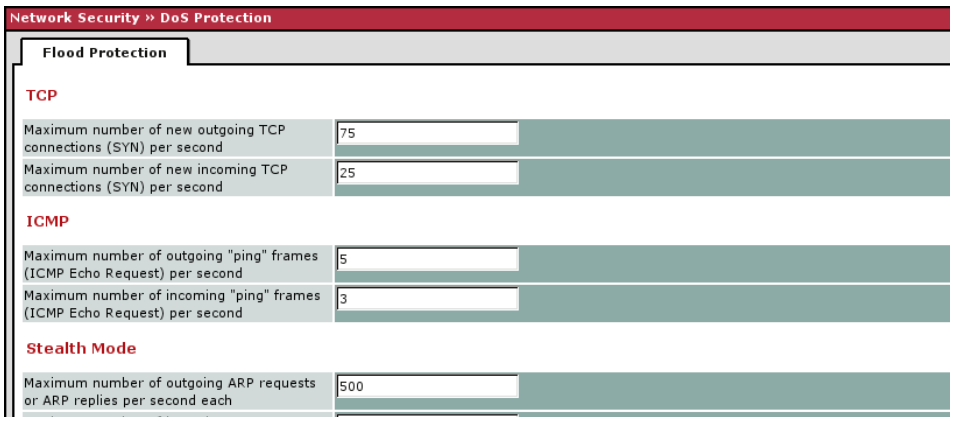
Network Security >> Packet Filter >> Advanced (Fortsetzung)		
	Allow TCP keepalive packets without TCP flags	TCP packets without flags set in their TCP header are normally rejected by the firewalls. At least one type of a Siemens control system with an older firmware sends TCP keepalive packets without TCP flags set; therefore, they are then rejected 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 6-140). 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** **ICMP via secondary 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 interface. 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 (Fortsetzung)		
	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 assigned 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 (Fortsetzung)		
	FTP	**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.
	H.323	**Yes/No, default: No** Protocol used to establish communication sessions between two or more participants. Used for audio-visual transmission. This protocol is older than SIP.
	SIP	**Yes/No, default: No** SIP (Session Initiation Protocol) is used to establish communication sessions between two or more participants. 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 communication 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.

6.6.2 Network Security >> DoS Protection

6.6.2.1 Flood Protection



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.
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 in or out.

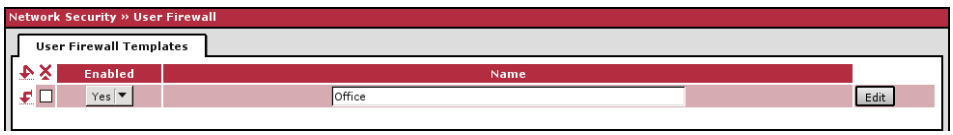
Network Security >> DoS Protection >> Flood Protection (Fortsetzung)		
Stealth Mode	**Maximum number of incoming/outgoing ARP requests or ARP replies per second each**	Default setting: 500 Maximum values for the number of incoming and outgoing ARP requests allowed per second. These values are set to 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.

6.6.3 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 6-113).

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

6.6.3.1 User Firewall Templates



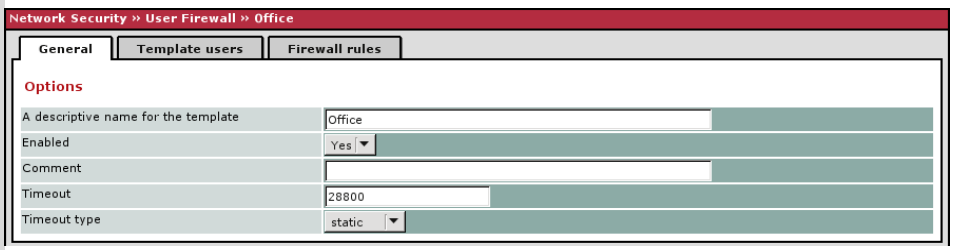
All defined user firewall templates are listed here. A template can consist of several firewall rules. A template can be assigned to several users.

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		
	Enabled	Activates/deactivates the relevant template.
	Name	Name of the template. The name is specified when the template is created.
General	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 user firewall rules 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 (Fortsetzung)

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.

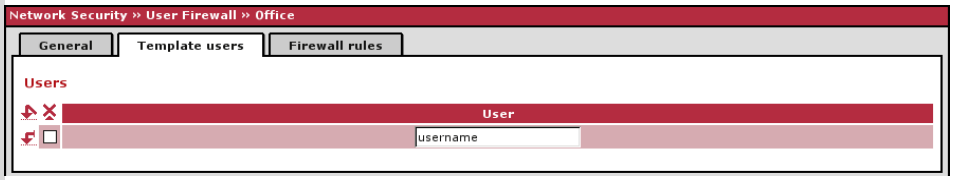
An FL MGUARD connection is considered to have expired if no more data is sent for this connection over the following periods.

Connection expiration period after non-usage

– TCP 5 days (this value can be set, see 6-140.)
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

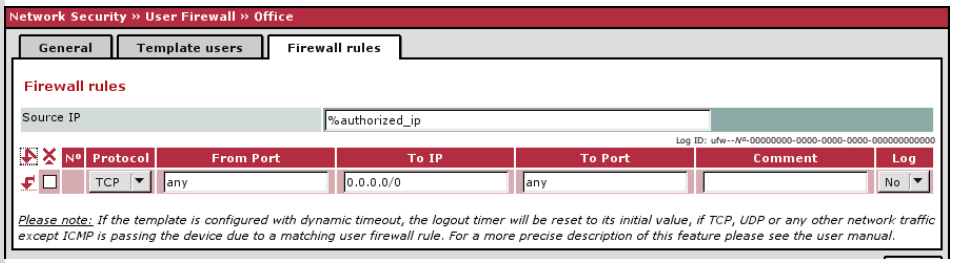
Network Security >> User Firewall >> User Firewall Templates Edit >> > ...

Template users



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 6-113).

Firewall rules



Source IP

IP address from which connections are allowed to be established. If this is to be the address from which the user logged into the FL MGUARD, the placeholder "%authorized_ip" should be used.

If multiple firewall rules are defined and activated for a user, 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, 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 6-220)

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)

6.7 CIFS Integrity Monitoring menu

This menu is **not** available on the **FL MGUARD BLADE** controller.

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 anti-virus 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 6-148).
– What type of access is permitted (see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings” on page 6-150).
– At what intervals the drives should be checked (see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit” on page 6-151).
– Which file types should be checked (see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Filename Patterns” on page 6-153).
– Warning method when a change is detected (e.g., via e-mail, see “CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings” on page 6-150 or via SNMP, see “CIFS integrity traps” on page 6-45).

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 6-148).
– What type of access is permitted (read or read/write access, see “CIFS Integrity Monitoring >> CIFS AV Scan Connector” on page 6-158).

6.7.1 CIFS Integrity Monitoring >> Importable Shares

Requirements

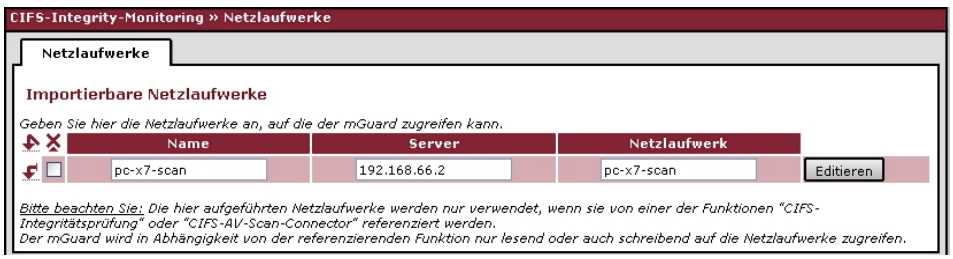
The network drives that the FL MGUARD should check regularly can be specified here.

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).

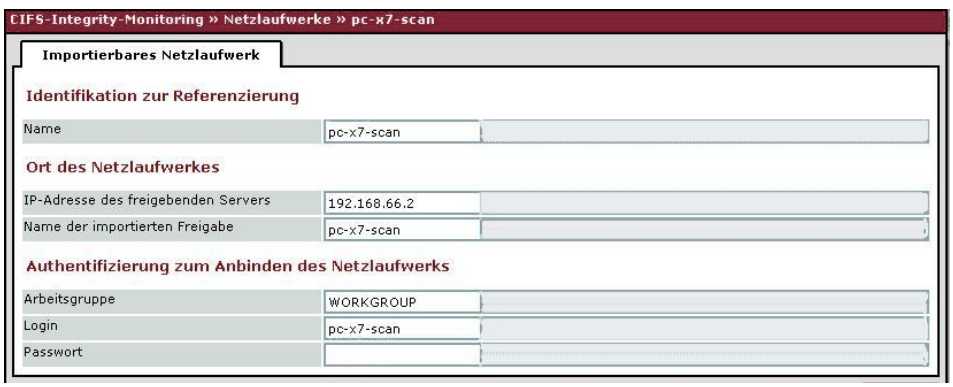
The references to the network drives can be set as follows:

– For CIFS integrity checking, see “Checked CIFS Share” on page 6-150.
– For CIFS anti-virus scan connector, see “CIFS Antivirus Scan Connector” on page 6-158.

6.7.1.1 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 authorized server.
	Share	Name of the network drive made available by the authorized 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 authorized server**	IP address of the server whose network drive is to be checked.

CIFS Integrity Monitoring >> Importable Shares >> Edit (Fortsetzung)		
Authentication for mounting the Share	**Imported share's name**	Directory on the above authorized server that is to be checked.
	Workgroup	Name of the workgroup to which the network drive belongs.
	Login	Login for the server.
	Password	Password for login.

6.7.2 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

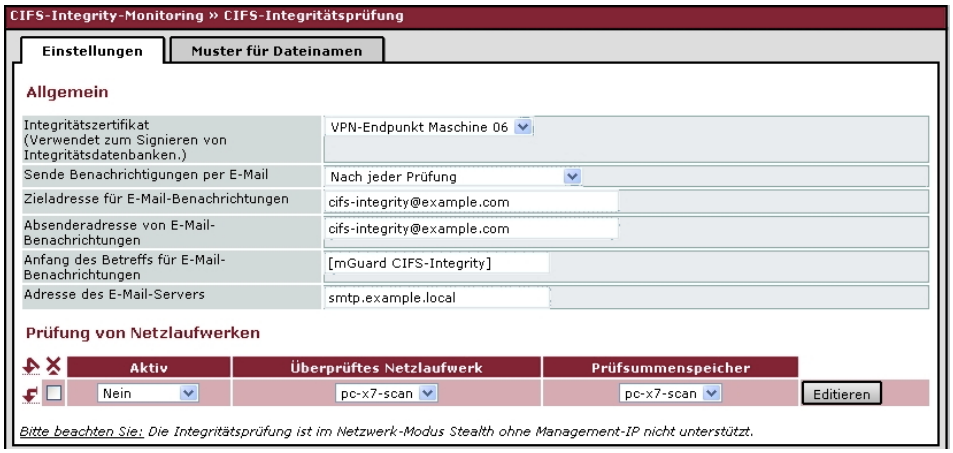
If a network drive that is to be checked is reconfigured, an integrity database must be created.

This integrity 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 6-156) or on the first regular check of the drive.

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.

6.7.2.1 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 6-123.
	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*).

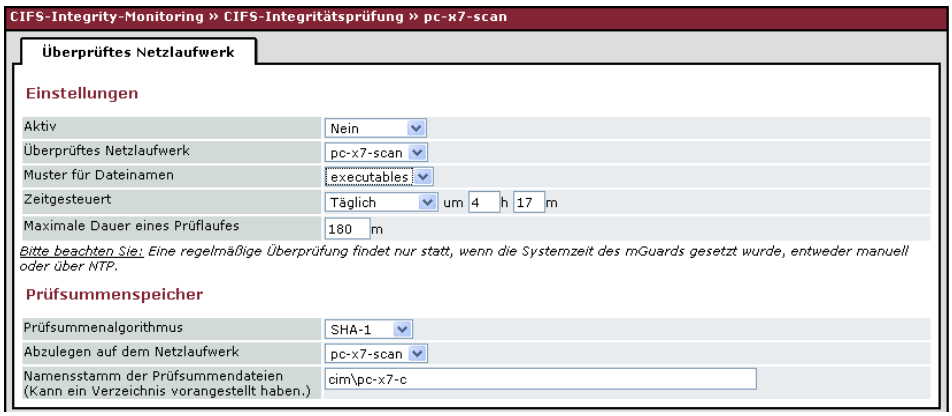
CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings (Fortsetzung)

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* .

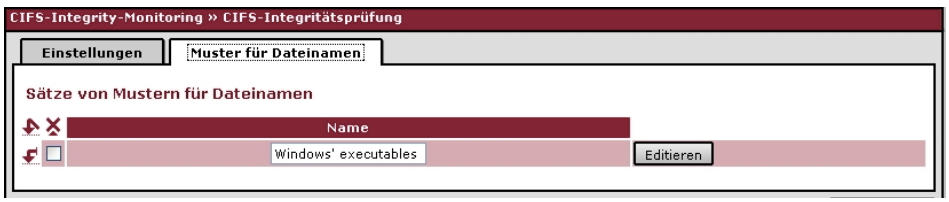
Do not check files that are changed in normal operation, as this could trigger false alarms.

Do not check files that are simultaneously opened **exclusively** by other programs, as this can lead to access conflicts.

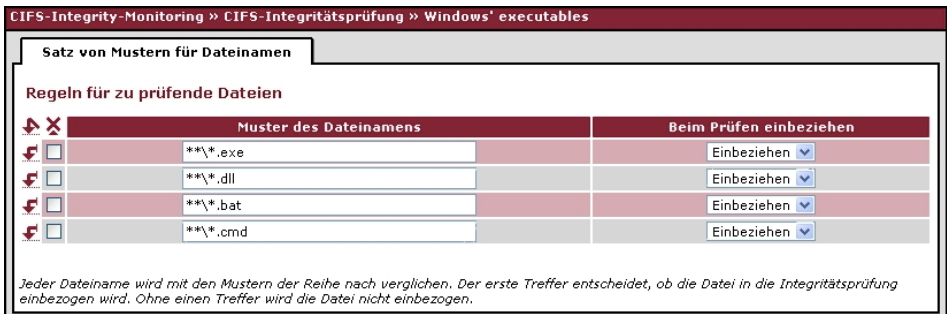
CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit (Fortsetzung)		
	Time Schedule	Everyday, Mondays, Tuesdays, etc. at xx h, xx m You can start a check every day or on a specific weekday at a specific time (hours, minutes). The FL MGUARD system time must be set for the time schedule 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 6-7). 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 6-156).
	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.

CIFS Integrity Monitoring >> CIFS Integrity Checking >> Settings >> Edit (Fortsetzung)		
	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 6-156).
	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".

6.7.2.2 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 template 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 placeholder (*) is permitted per directory or file name.

Placeholders 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.

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 templates one after the other. The first hit is decisive for the inclusion of the file in the integrity check. The file is not included if no hits are found.)

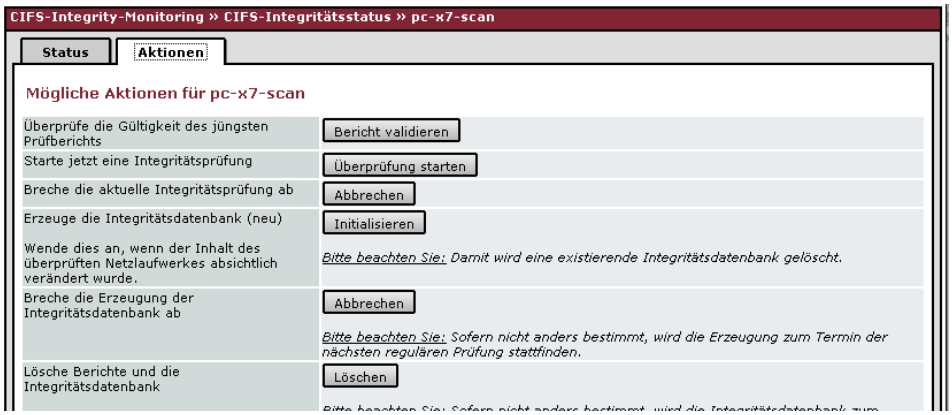
Exclude: The files are excluded from the check.

6.7.3 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 6-151).
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 (Fortsetzung)		
	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 6-156. (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 (Fortsetzung)

(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.

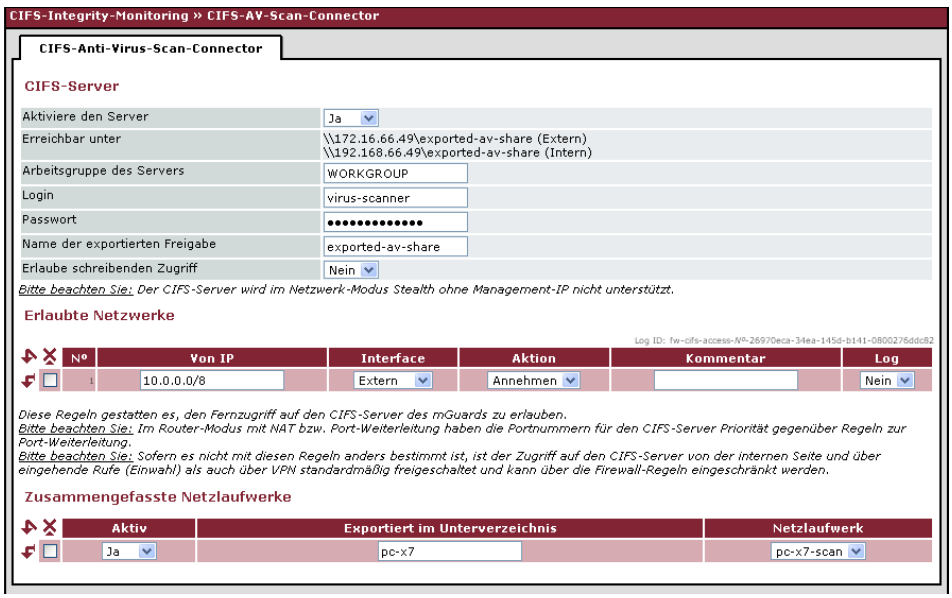
6.7.4 CIFS Integrity Monitoring >> CIFS AV Scan Connector

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 anti-virus 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.

6.7.4.1 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 (Fortsetzung)		
	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 (see“Accessing the virtual network (CIFS Antivirus Scan Connector)” on page 6-161). 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 when access should be made over the external interface. 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 6-88).
	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 should 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 IP addresses. To specify an address area, use CIDR format (see 6-220)

CIFS Integrity Monitoring >> CIFS AV Scan Connector (Fortsetzung)		
	Interface	**External/Internal/External 2/VPN/Dial-in**[1] Specifies to which interface the rules 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, so the sender is informed of their rejection. (In *stealth* mode, Reject has the same effect as Drop.) **Drop** means that the data packets may not 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 6-57).

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 "Extras, Map network drive..." menu in Windows Explorer and enter the path with 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

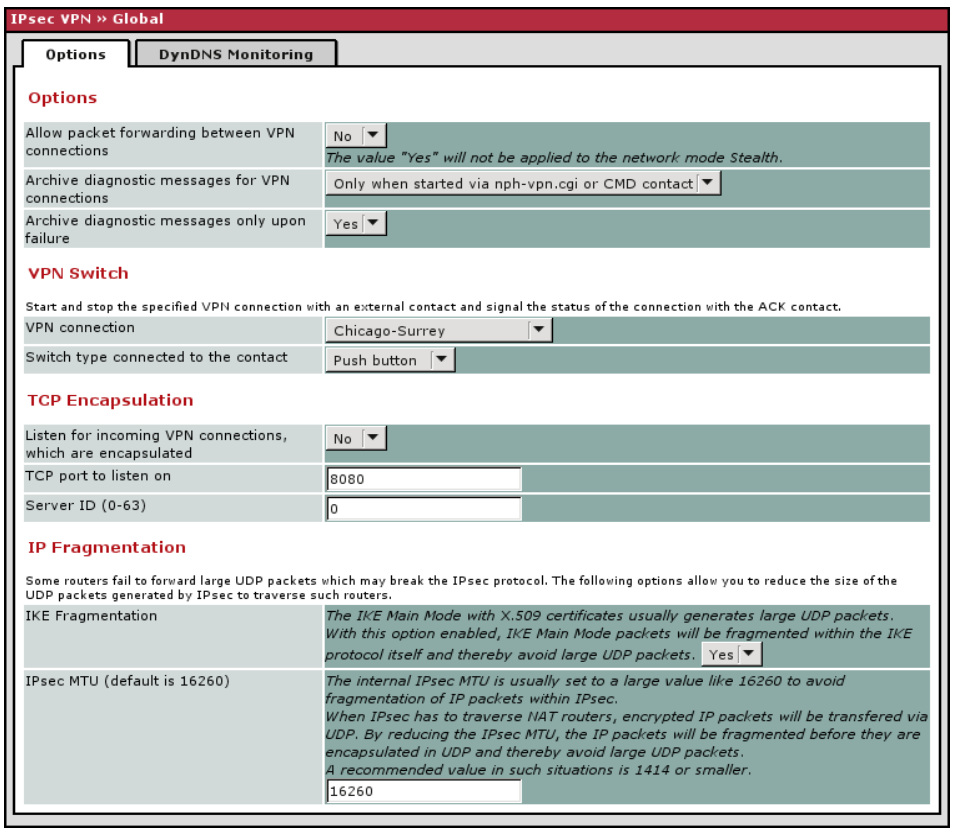
– DNS names can also be used instead of the IP address.
– The authorized network cannot be found using the browse or search function.
– The "Exported share's name" must always be added.
– Windows does not automatically display the authorized network upon connection of the FL MGUARD.

6.8 IPsec VPN menu

This menu is **not** available on the **FL MGUARD BLADE** controller.

6.8.1 IPsec VPN >> Global

6.8.1.1 Options



IPsec VPN >> Global >> Options

Options

Allow packet forwarding between VPN connections

This option should only be set to **Yes** on an FL MGUARD communicating between two different VPN remote peers.

To enable communication between two VPN remote peers, the local network of the communicating FL MGUARD must be configured so that the remote networks containing the VPN remote peers are included. The opposite setup (local and remote network swapped round) must also be implemented for VPN remote peers (see “Remote” on page 6-176).

Yes is not supported in *stealth* network mode.

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 remote peers 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 remote peers (see “Authentication” on page 6-183).

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 RS.

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:

IPsec VPN >> Global >> Options (Fortsetzung)

– In certain application environments, e.g., when the FL MGUARD is "operated" by means of a machine control system via the CMD contact (FL MGUARD RS ... 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 remote peer, 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 www.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 the Innominate Support team with additional options for more efficient troubleshooting than would be possible without archiving.

Archive diagnostic messages only upon failure: Yes/No	Only visible if archiving is enabled. If only log entries generated for failed connection attempts should be archived, set this option to **Yes**. If set to **No**, all log entries will be archived.

IPsec VPN >> Global >> Options (Fortsetzung)

VPN Switch

Only for FL MGUARD RS ...

VPN connection

The FL MGUARD RS ... has connections to which an external pushbutton or on/off switch and a signal LED can be connected. One of the configured VPN connections can be established and released via the pushbutton 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 6-170), they are displayed in this selection list. Select here if the connection is to be established or released manually by pressing the pushbutton or switch.

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 pushbutton 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.

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.

Only for FL MGUARD RS ...

Switch type connected to the contact

Push button or on/off switch

The FL MGUARD RS ... has connections to which an external pushbutton or on/off switch and a signal LED can be connected. Select the switch type that is connected to the corresponding service contacts of the FL MGUARD RS ...,
For additional information, see “Installing the FL MGUARD RS ...” on page 4-4 or under **Service Contacts**. Information about how to operate the different switch types is also described.

If a VPN connection is established by pressing the pushbutton or switch, the connection is maintained until it is released by pressing the pushbutton or switch again.

If an on/off switch is used (instead of a pushbutton) 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 can accept VPN connections encapsulated in TCP, even when the FL MGURAD is positioned behind a NAT gateway in the network and thus cannot be reached by the VPN remote peer 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 6-167).

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

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.

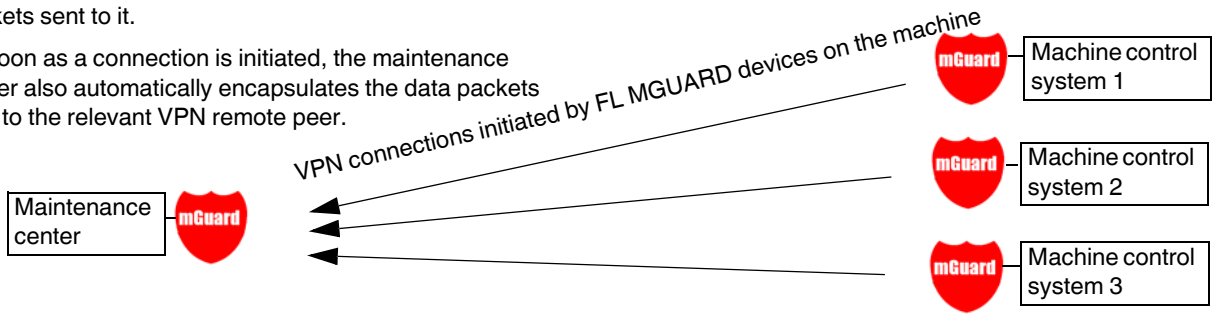
If the FL MGUARD is configured to use a proxy for HTTP and HTTPS in the "Network >> Proxy Settings" menu item, then this proxy is also used for VPN connections that use TCP encapsulation.

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

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 remote peer.



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 remote site's VPN gateway: **%any**
  Connection startup: **Wait**

FL MGUARD devices on machine control systems

Required basic settings

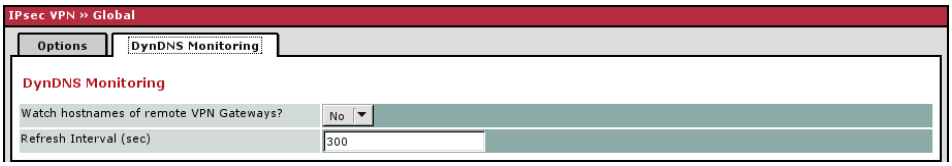
- **IPsec VPN** menu item**,** ***Global, Options*** tab page:
  Listen for incoming VPN connections, which are encapsulated: **No**
- *Connections* submenu, *General* tab page:
  Address of the remote site's VPN gateway: Fixed IP address or host name
  Connection startup: **Initiate** or **Initiate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

Figure 6-2 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 the FL MGUARD can accept connection establishment with encapsulated packets. For technical reasons, the main memory (RAM) requirements increase with each interface that needs to be listened on for VPN connections encapsulated in TCP. If multiple interfaces need to be listened on, then the device must have at least 64 Mbytes RAM. The interfaces to be listened on are determined by the FL MGUARD according to the settings on the active VPN connections that have configured "%any" as the remote peer. The decisive setting is specified under "Interface to use for gateway setting %any".

IPsec VPN >> Global >> Options (Fortsetzung)		
	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 remote peer 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 listen in on must not be identical to a port that is being used for remote access (SSH, HTTPS or SEC stick).
	Server ID (0-63)	Usually, the default value **0** does not have to be changed. The numbers are used to differentiate between different 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, then the transmission of small UDP packets should be agreed upon first. 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**. 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.

6.8.1.2 DynDNS Monitoring



For an explanation on DynDNS, see “DynDNS” on page 6-105.

IPsec VPN >> Global >> Options		
DynDNS Monitoring	**Watch hostnames of remote VPN Gateways?**	**Yes/No** If the FL MGUARD knows the address of a VPN remote peer in the form of a host name (see “Defining a VPN connection/VPN connection channels” on page 6-172) 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

6.8.2 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.

– In order to successfully establish an IPsec connection, the VPN remote peer 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 or SHA-1 hash algorithms
  – Tunnel or transport mode
  – Quick mode
  – Main mode
  – SA lifetime (1 second to 24 hours)

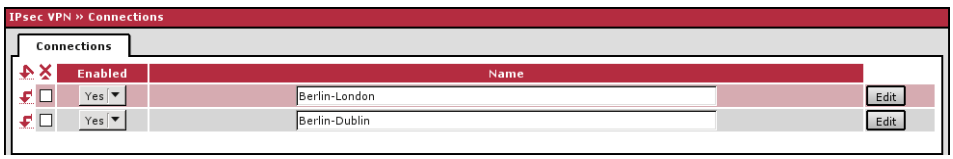
  If the remote peer is a computer running Windows 2000, the *Microsoft Windows 2000 High Encryption Pack* or at least Service Pack 2 must be installed.
– If the remote peer is positioned downstream of a NAT router, the remote peer must support NAT-T. Alternatively, the NAT router must know the IPsec protocol (IPsec/VPN passthrough). For technical reasons, only IPsec tunnel connections are supported in both cases.

6.8.2.1 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.



6.8.3 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 MGUARD192.168.1.1/nph-vpn.cgi?name=Athen&cmd=up"
```

The `--no-check-certificate` option ensures that the HTTPS certificate on the FL MGUARD is not checked further. It may be necessary to code the password for the URL if it contains special characters. A command like this relates to all connection channels that are summarized 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 address 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:

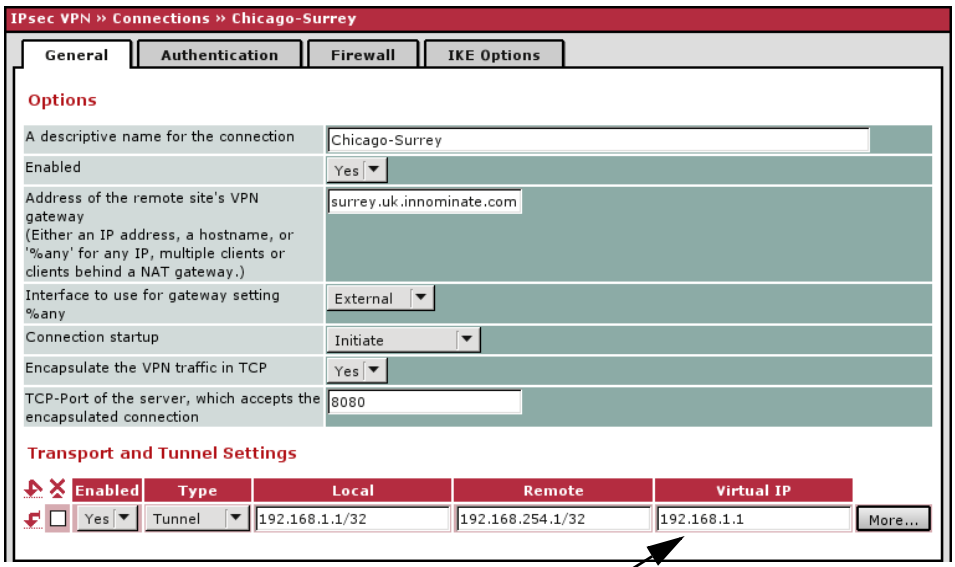
Table 6-1 Status of a VPN connection

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 remote peer 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.
`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**.

6.8.3.1 General



IPsec VPN >> Connections >> Edit >> General		
Options	**A descriptive name for the connection**	The connection can be freely named and 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 6-183) – 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 remote peers or remote peers downstream of a NAT router.

Address of the remote site's VPN gateway

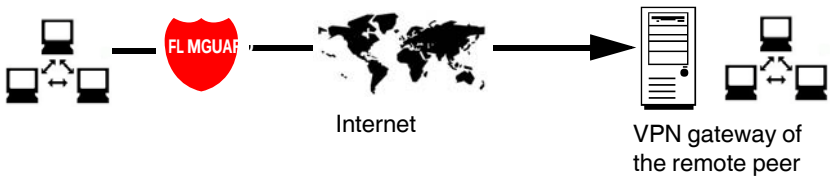


Figure 6-3 The address of the transition to the private network where the remote communication partner is located

– If the FL MGUARD should actively initiate and establish the connection to the remote peer, specify the IP address or host name of the remote peer here.
– If the VPN gateway of the remote peer 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 accept a connection to the local FL MGUARD that was actively initiated and established by a remote peer 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 peer if this remote peer 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" peer has a fixed and known IP address.

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

If locally stored CA certificates are to be used to authenticate the remote peer, the address of the VPN gateway of the remote peer 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 with "%any"), then a VPN identifier (see “VPN Identifier” on page 6-186) must be specified.

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

If **TCP Encapsulation** is used (see “TCP Encapsulation” on page 6-166):
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 send encapsulated data packets, **%any** must be specified for the VPN gateway of the remote peer.

IPsec VPN >> Connections >> Edit >> General		
Options	**Interface used for the "%any" gateway setting**	**Internal, External, External 2, Dial-in** *External 2* and *Dial-in* are only for devices with a serial interface, see “Network >> Interfaces” on page 6-57. 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 remote peer. 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 be made over a specific interface for VPN remote peers without a known IP address. If an IP address or hostname is entered for the remote peer, 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 are 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 remote peer.
	Connection startup: Initiate/Initiate on traffic/Wait	**Initiate** The FL MGUARD initiates the connection to the remote peer. In the *Address of the remote site's VPN gateway* field (see above), the fixed IP address of the remote peer 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 accept the connection to the FL MGUARD that a remote peer actively initiates and establishes.  If **%any** is entered under *Address of the remote site's VPN gateway*, **Wait** must be selected.

IPsec VPN >> Connections >> Edit >> General (Fortsetzung)

Encapsulate the VPN traffic in TCP

Yes/No (default: No)

If the **TCP Encapsulation** function is used (see “TCP Encapsulation” on page 6-166), 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 remote peer 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 remote peer. The port number specified here must be the same as the one specified for the FL MGUARD of the remote peer under **TCP port to listen on** (*IPsec VPN* >> *Global* >> *Options* menu item).

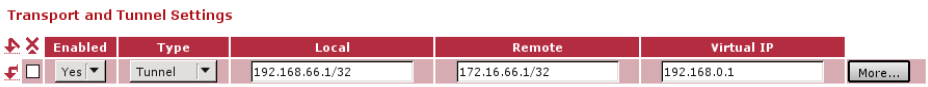
If TCP Encapsulation is used (see page 6-166):

– 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 (Fortsetzung)

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, sent to the VPN gateway of the remote peer – the "tunnel end". The transmitted datagrams are then decrypted and the original datagrams are restored. These are then forwarded to the destination computer.

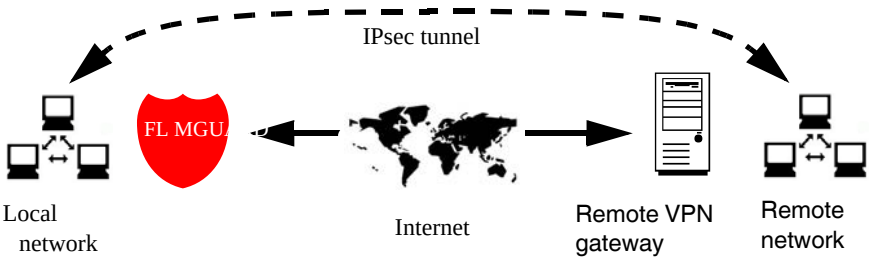
Transport (host ↔ host)

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 that 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 6-172) is specified as **%any**, it is possible that a number of different remote peers will connect to the FL MGUARD.

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.

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)*

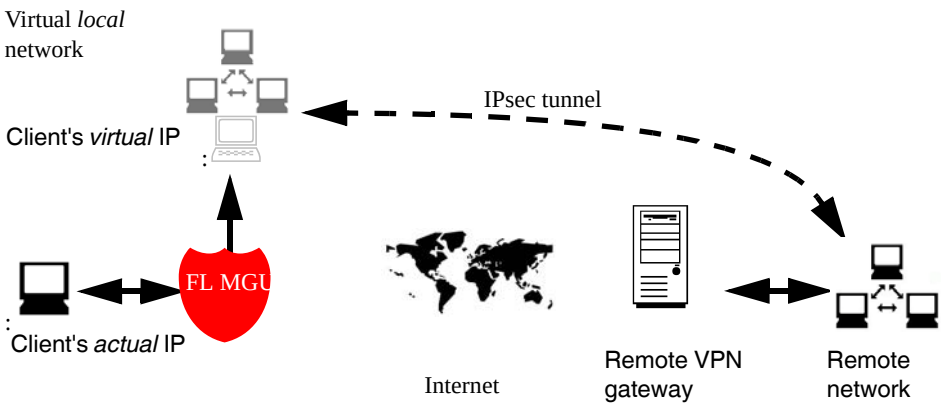


Figure 6-4 Virtual IP

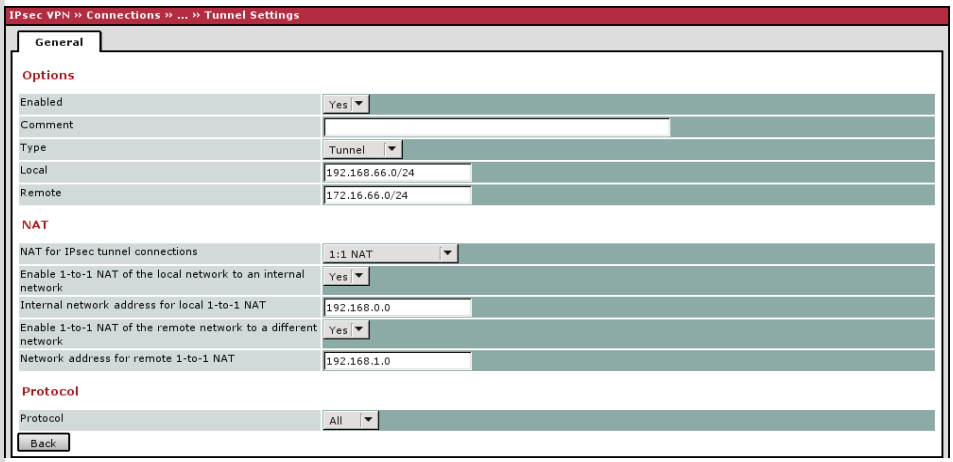
In *stealth* mode, the local network of the VPN is simulated by the FL MGUARD. Within this *virtual* network, the client is known as and can be addressed by the *virtual* IP address to be entered here.

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 6-176

Remote See “Remote” on page 6-176

Virtual IP for the client See “Virtual IP address (only in stealth mode)” on page 6-178

NAT

NAT for IPsec tunnel connections **Off/Local masquerading/1:1 NAT**

Default: **Off**

Local masquerading

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" so that this signifies exactly one IP address.

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 6-57).

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

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:

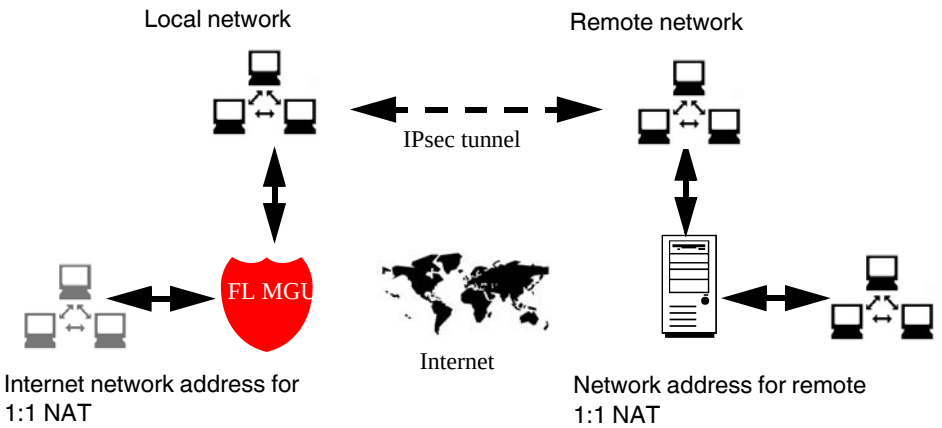


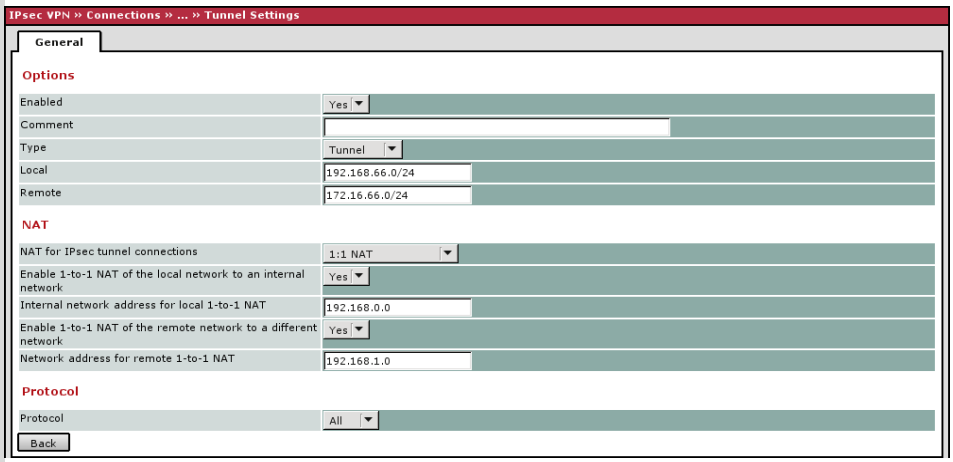
Figure 6-5 1:1 NAT

IPsec VPN >> Connections >> Edit >> General

Further settings can be made by clicking on **More...**

Options

Tunnel connection type



NAT

Enable 1-to-1 NAT of the local network to an internal network

Yes/No

Rewrites the local network specified under *Local* to an actual existing local network.
This option is set to **No** by default.

Internal network address for local 1-to-1 NAT

(Only if **Yes** has been selected above.)

The actual network address of the system in the local network.
The subnet mask is taken from the **Local** field.

Enable 1-to-1 NAT of the remote network to a different network

Rewrites the remote network agreed by the VPN remote peer under *Remote* as if the computers connected there and their addresses were located in another network.

This option is set to **No** by default.

Network address for remote 1-to-1 NAT

(Only if **Yes** has been selected above.)

The remote network address actually addressed by the systems in the local network.
The subnet mask is taken from the *Remote* field.

If the *remote network* or the *remote network for 1:1 NAT* are within one of the networks directly connected to the LAN port of the FL MGUARD, the FL MGUARD will also answer ARP requests for IP addresses within the remote network.
This allows access to a remote VPN using local IP addresses without changing the routing of locally connected clients.

IPsec VPN >> Connections >> Edit >> General (Fortsetzung)

Further settings can be made by clicking on **More...**

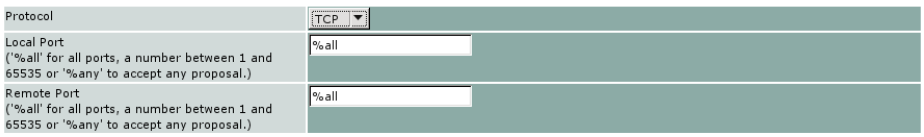
Protocol

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:



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

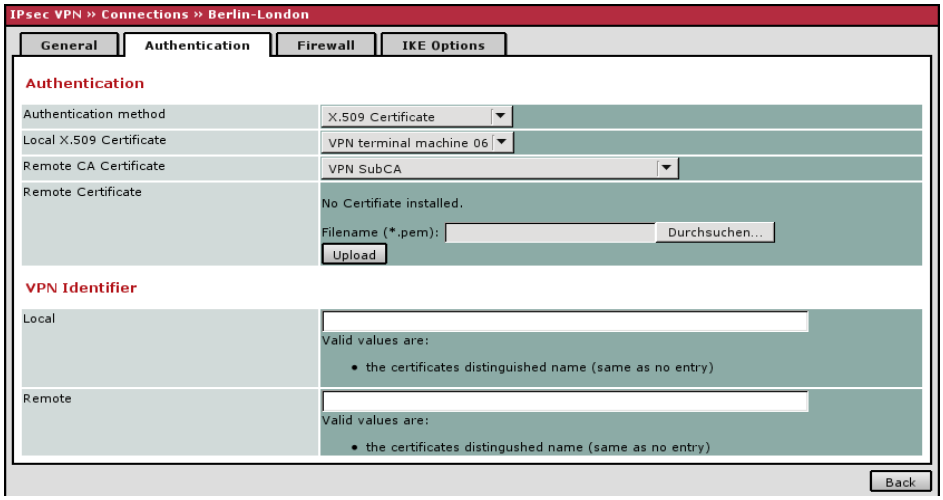
%all (default) specifies that all ports can be used. If a specific port should be used, specify the port number.

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

6.8.3.2 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.

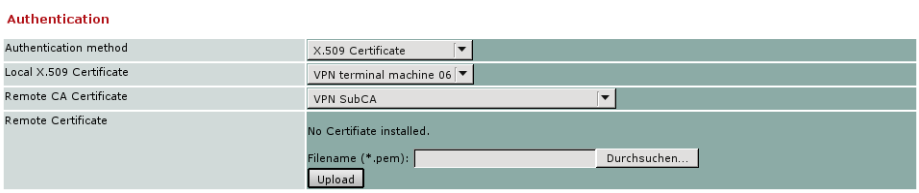
Authentication method: X.509 Certificate

This method is supported by most modern IPsec implementations. With this option, each VPN device has a private key and a public key in the form of an X.509 certificate, which contains additional information about the certificate's owner and the certification authority (CA).

The following must be specified:

– How the FL MGUARD authenticates itself to the remote peer
– How the FL MGUARD authenticates the remote peer

How the FL MGUARD authenticates itself to the remote peer



IPsec VPN >> Connections >> Edit >> Authentication

Local X.509 Certificate

Specifies which machine certificate the FL MGUARD uses as authentication to the VPN remote peer.

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 6-116).

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 peer

The following definition relates to how the FL MGUARD verifies the authenticity of the VPN remote peer.

The table below shows which certificates must be provided for the FL MGUARD to authenticate the VPN remote peer if the VPN remote peer 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 6-116.

Authentication for VPN

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

According to this table, the certificates that must be provided are the ones the FL MGUARD uses to authenticate the relevant VPN remote peer.

Requirement

The following instructions assume that the certificates have already been correctly installed on the FL MGUARD (see “Authentication >> Certificates” on page 6-116, apart from the remote certificate).

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 remote peer must be checked for revocations. This excludes locally configured (imported) remote certificates.

Remote CA Certificate

Self-signed machine certificate

If the VPN remote peer 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 6-185).

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 remote peer authenticates itself with a machine certificate **signed by a CA**:

It is possible to authenticate the machine certificate shown by the remote peer 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 remote peer 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 remote peer 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 remote peers 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 6-185).

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 remote peer should 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 remote peer is authenticated using CA certificates.

VPN gateways use the *VPN identifier* to determine which configurations belong to the same VPN connection.
If the FL MGUARD consults CA certificates to authenticate a VPN remote peer, 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 remote peer. 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 remote peer for the FL MGUARD to accept this VPN remote peer as a communication partner.

It is then possible to limit or enable access by VPN remote peers, 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*

(see “Subject, certificate” on page 8-5)

"Distinguished Name" was previously used instead of "Subject".

IPsec VPN >> Connections >> Edit >> Authentication (Fortsetzung)

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 remote peer. 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 end point 01, O=example GmbH, C=US

If certain subject attributes have very specific values for the acceptance of the VPN remote peer 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=example GmbH, C=US
(with or without spaces between attributes)

In this example, the attributes "O=example GmbH" 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.

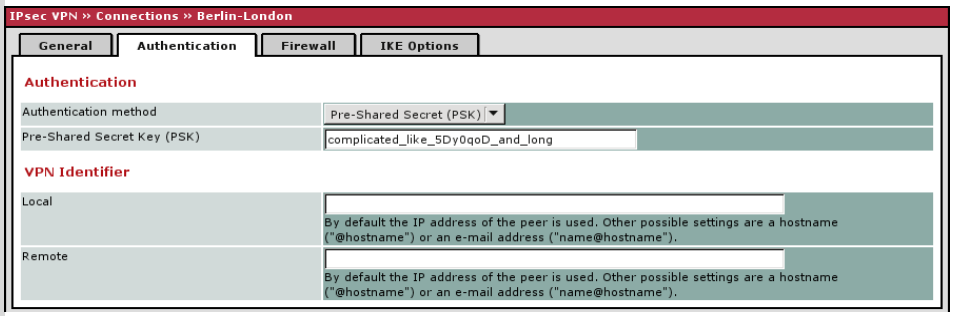
If a subject filter is set, the number **and** the order of the specified attributes must correspond to that of the certificates for which the filter is to be used.

Please note these are case-sensitive.

IPsec VPN >> Connections >> Edit >> Authentication (Fortsetzung)

VPN Identifier

Authentication method: Pre-Shared Key (PSK)



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 Key (PSK)** entry field.

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.

Pre-Shared 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.

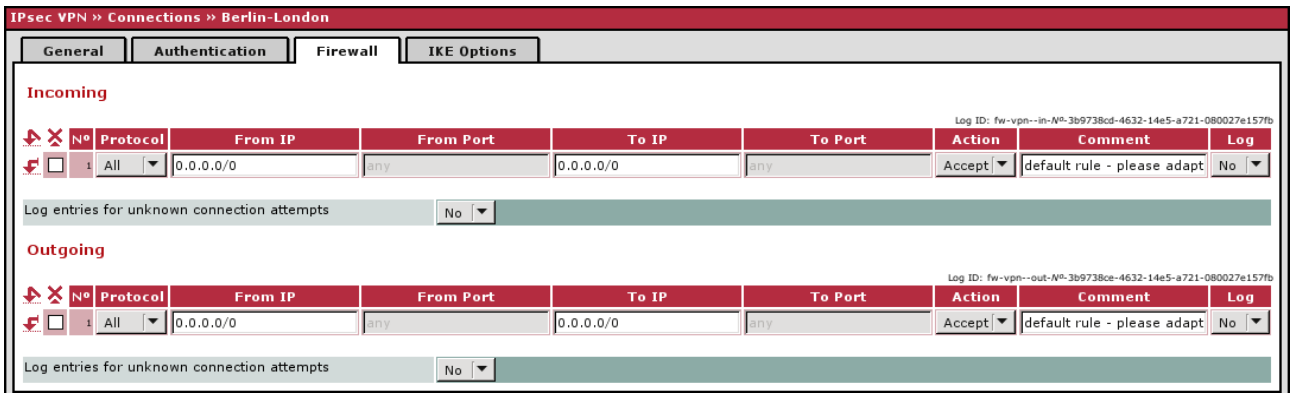
Pre-Shared Key cannot be used if at least one (or both) of the communication partners is located downstream of a NAT gateway.

VPN gateways use the *VPN identifier* to determine 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 names with "@" prefix (e.g., "@vpn1138.example.com")
– An e-mail address (e.g., "piepiorra@example.com")

6.8.3.3 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 6-130), 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.

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 6-130, “Network Security >> Packet Filter” on page 6-130, “Advanced” on page 6-138).

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.

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.

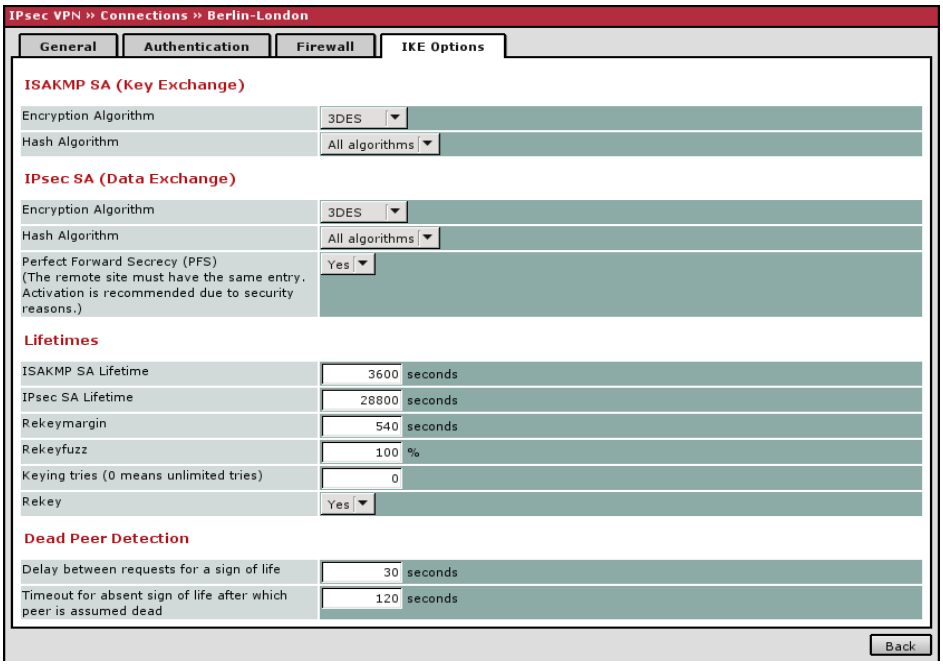
If the *Allow packet forwarding between VPN connections* option is set to **Yes** on the *Global* tab page, the rules under **Incoming** are used for the incoming data packets to the FL MGUARD, and the rules under **Outgoing** are applied to the outgoing data packets.

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.

IPsec VPN >> Connections >> Edit >> Firewall		
Incoming	**Protocol**	**All** means TCP, UDP, ICMP, 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 6-220) **Incoming:** – From IP: The IP address in the VPN tunnel – To IP: The 1:1 NAT address or the real address **Outgoing**: – From IP: The 1:1 NAT address or the real 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, so the sender is informed of their rejection. (In *stealth* mode, Reject has the same effect as Drop.) **Drop** means that the data packets may not 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	When set to **Yes**, all connection attempts that are not covered by the rules defined above are logged.

6.8.3.4 IKE Options



IPsec VPN >> Connections >> Edit >> IKE Options

ISAKMP SA (Key Exchange)

Encryption Algorithm

Decide on which encryption method should be used with the administrator of the remote peer.

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 not used that widely yet.

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 remote peer.

The algorithm designated as "Null" does not contain encryption.

Hash Algorithm

Leave this set to *All algorithms*. It then will not make a difference whether the remote peer is operating with MD5 or SHA-1.

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.

IPsec VPN >> Connections >> Edit >> IKE Options		
	Encryption Algorithm	See above.
	Hash Algorithm	See above.
	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. Only select **Yes** if the remote peer supports PFS. Set *Perfect Forward Secrecy (PFS)* to **No** if the remote peer is an IPsec/L2TP client.
Lifetimes	**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 the 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).
	Rekeymargin	Minimum time period before the old key expires, and during which a new key should be created. Default setting: 540 seconds (9 minutes).
	Rekeyfuzz	Maximum amount as a percentage by which the *rekey margin* should be randomly increased. 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 remote peer. 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 remote peer 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	Period of time in seconds after which *DPD Keep Alive* requests should be sent. 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	Period of time in seconds after which the connection to the remote peer 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).

6.8.4 IPsec VPN >> L2TP over IPsec

These settings are not applied in stealth mode.

Allows VPN connections to the FL MGUARD to be established using the IPsec/L2TP protocol.

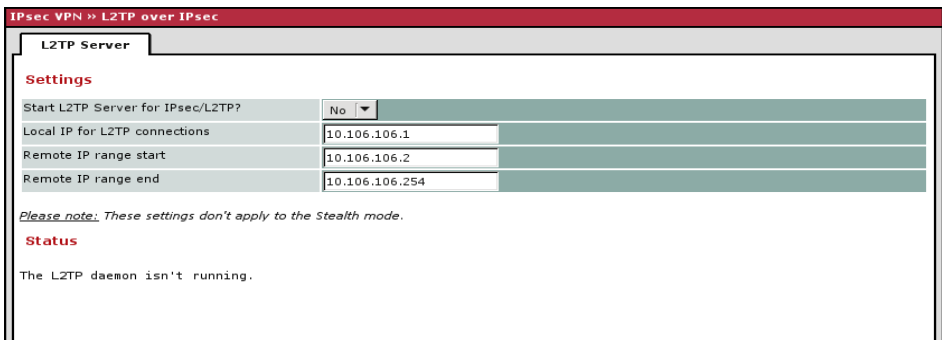
In doing so, the L2TP protocol is driven using an IPsec transport connection in order to establish a tunnel connection to a Point-to-Point Protocol (PPP). Clients are automatically assigned IP addresses by the PPP.

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

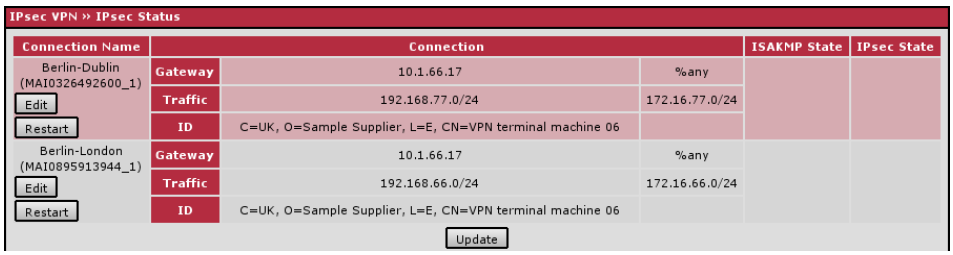
(See also "Further settings can be made by clicking on **More...**" on page 6-179 and “IKE Options” on page 6-191.)

6.8.4.1 L2TP Server



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 remote peer 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 remote peer 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.

6.8.5 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 release 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, all the data under "IPsec SA" and "Tunnel Settings" is correct.

In the event of problems, it is recommended that you check the VPN logs of the remote peer 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 correspond 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 remote peer is causing problems. In this case, deactivate and reactivate the connection to reestablish the connection.

6.9 SEC-Stick menu

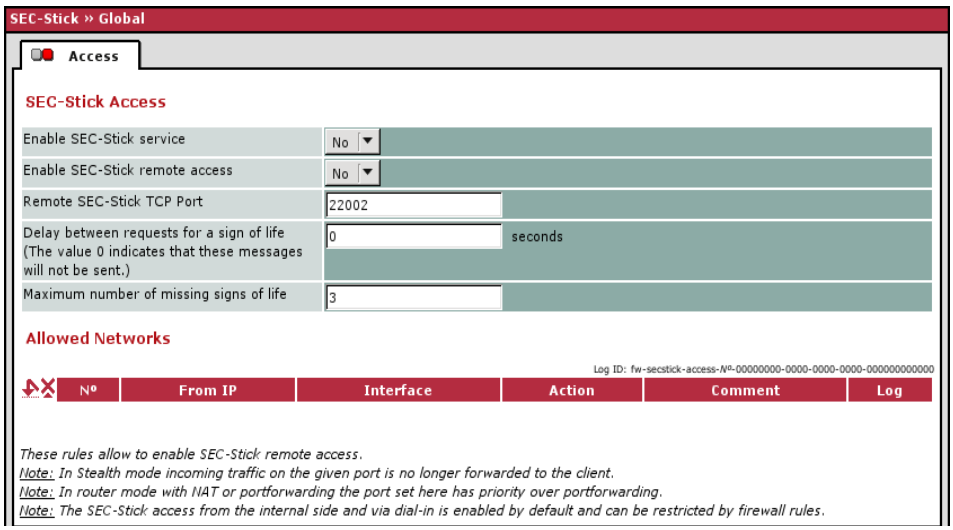
The FL MGUARD supports the use of an SEC-Stick, which is an access protector for IT systems. The SEC-Stick is a product of the team2work company: www.team2work.de

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.

6.9.1 Global



SEC-Stick >> Global >> Access

SEC-Stick Access

Access via the SEC-Stick requires a license. This access function can only be used if the corresponding license has been purchased and installed.

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.

SEC-Stick >> Global >> Access (Fortsetzung)

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

The preset "0" means that no requests for a sign of life are sent.

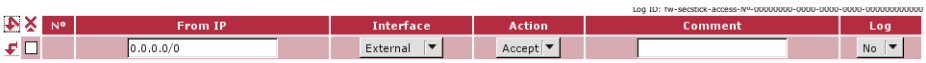
Positive values from 1 to 3600 can be set. They indicate that the FL MGUARD sends a request to the remote peer within the encrypted SSH connection to find out whether it can be accessed. The request is sent, if no activity was detected from the remote peer for the specified number of seconds (e.g., due to network traffic within the encrypted connection).

Maximum number of missing signs of life

Specifies the maximum number of times a sign of life request to the remote peer 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 when a sign of life is not detected after approximately 45 seconds.

Allowed Networks

Lists the firewall rules that have been set up. These apply for remote SEC-Stick access.



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

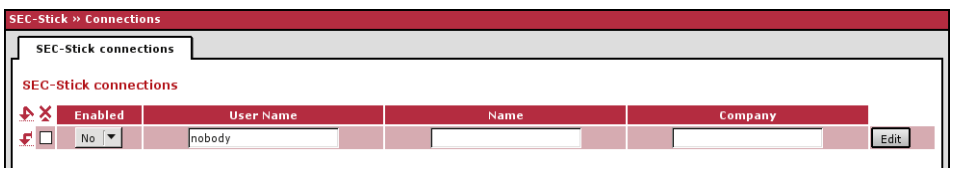
Enter the address of the computer/network from which remote access is permitted or forbidden in this field.

IP address **0.0.0.0/0** means all IP addresses. To specify an address area, use CIDR format (see 6-220)

SEC-Stick >> Global >> Access (Fortsetzung)		
	Interface	**External/Internal/External 2/VPN/Dial-in**[1] Specifies to which interface the rules 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. 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, so the sender is informed of their rejection. (In *stealth* mode, *Reject* has the same effect as *Drop*.) **Drop** means that the data packets may not 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)

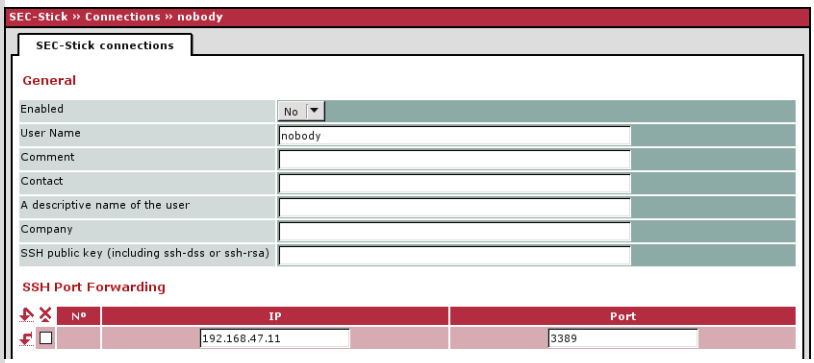
1 *External 2* and *Dial-in* are only for devices with a serial interface (see “Network >> Interfaces” on page 6-57).

6.9.2 Connections



SEC-Stick >> Connections >> SEC-Stick connections		
SEC-Stick connections	**List of defined SEC-Stick connections. Click on the down arrow in the top left, 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**.

SEC-Stick >> Connections >> SEC-Stick connections (Fortsetzung)		
	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 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.
	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.

6.10 QoS menu

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).

6.10.1 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.

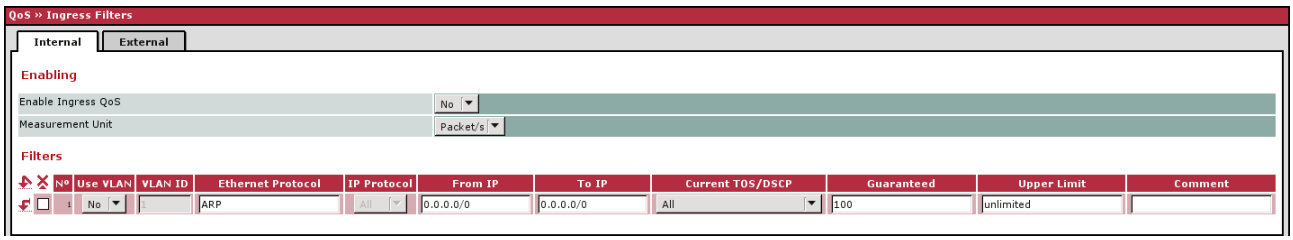
Using suitable filter rules, administrative access to the FL MGUARD can be ensured with high probability, for example.

Packet processing on the FL MGUARD is generally defined by the handling of individual data packets so that the processing performance depends on the number of packets and not on the bandwidth.

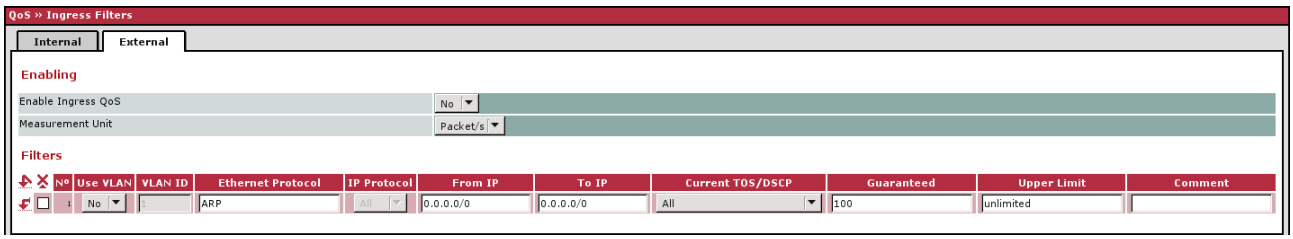
Filtering is performed exclusively according to characteristics that are present or may be present in each data packet: The sender and recipient IP address specified in the header, the specified Ethernet protocol, the specified IP protocol, the specified TOS/DSCP value and/or the VLAN ID (if VLANs have 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. This also applies to the entry of a sender or recipient IP address if the hexadecimal IPX Ethernet protocol is specified.

6.10.1.1 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. This option must be set to **Yes**.
	VLAN ID	Specifies that the VLAN data packets that have this VLAN ID may pass through. (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 (Fortsetzung)		
	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 6-220)
	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, then 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 will 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.
	Comment	Optional comment text.

6.10.2 Egress Queues

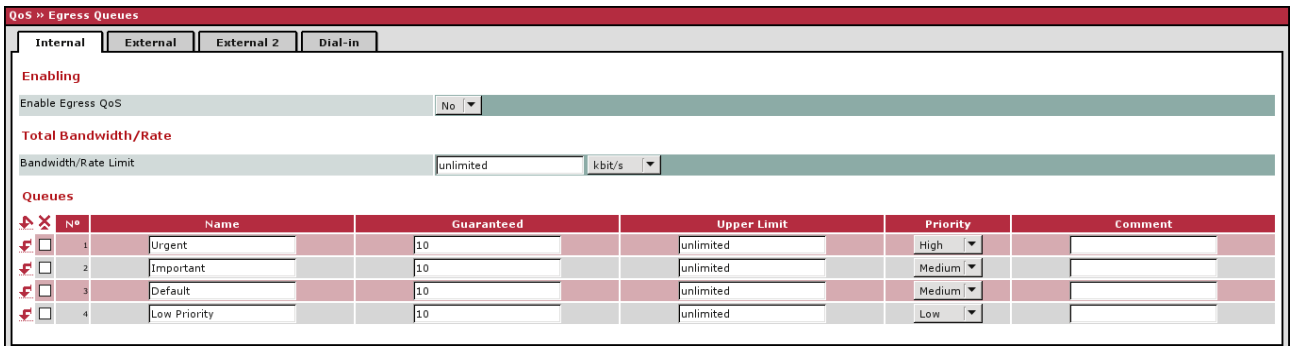
The services are assigned corresponding priority levels. In the event of connection bottlenecks, the outgoing data packets are placed in egress queues (i.e., queues for pending packets) according to the assigned priority level and are then processed according to their priority. Ideally, the assignment of priority levels and bandwidths should result in a sufficient bandwidth level always being available for the real-time 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.

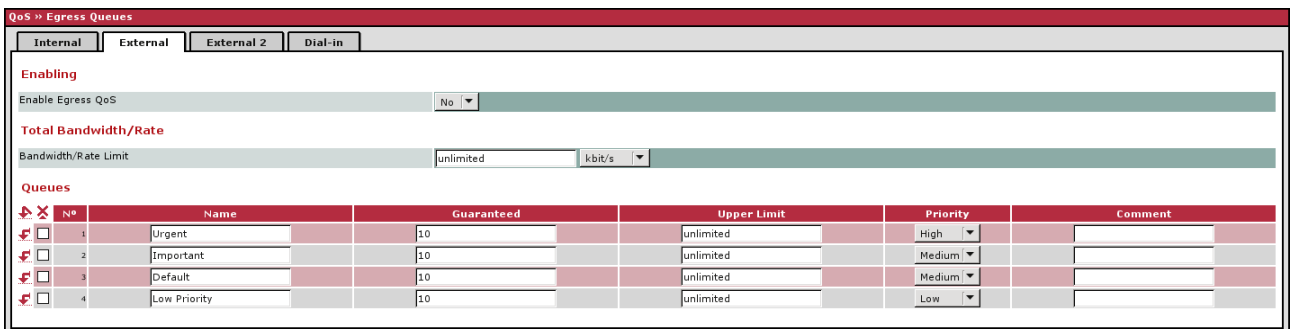
The *Egress Queues* feature can be used for all interfaces and for VPN connections.

6.10.2.1 Internal/External/External 2/Dial-in

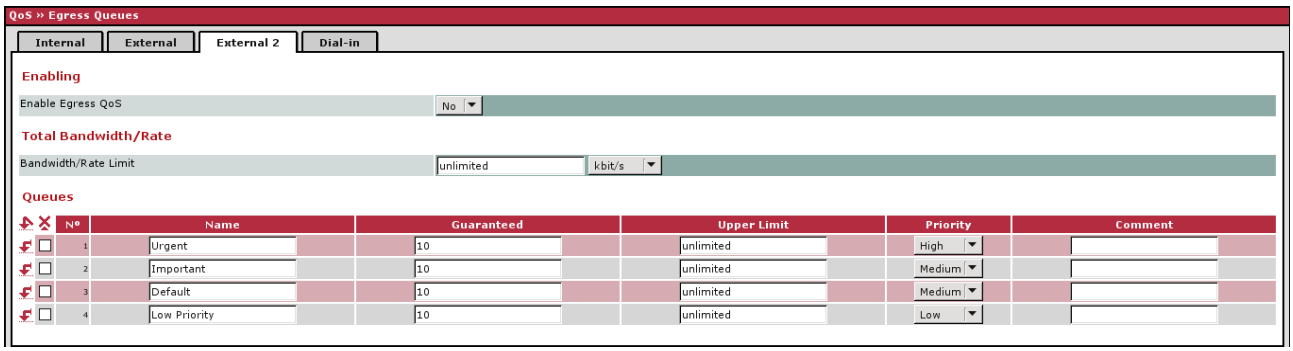
Internal: Settings for egress queues on the LAN interface



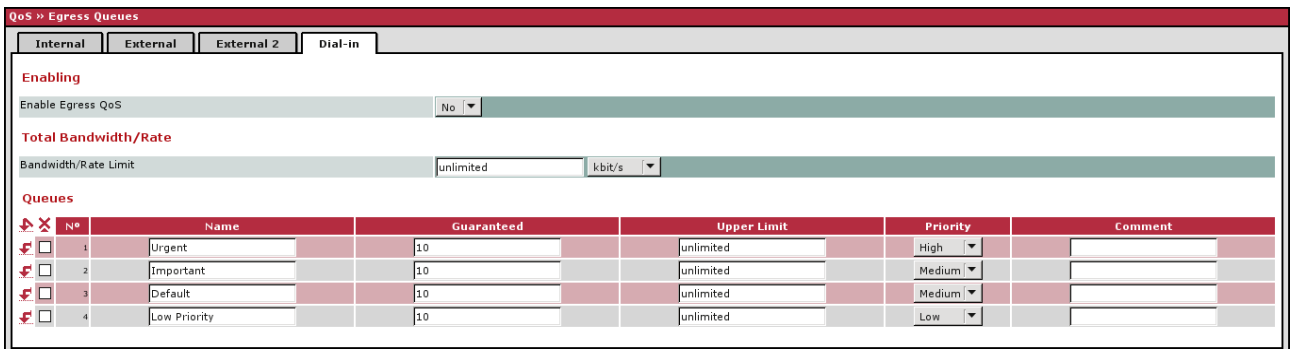
External: Settings for egress queues on the external WAN interface



External 2: Settings for egress queues on the secondary external interface



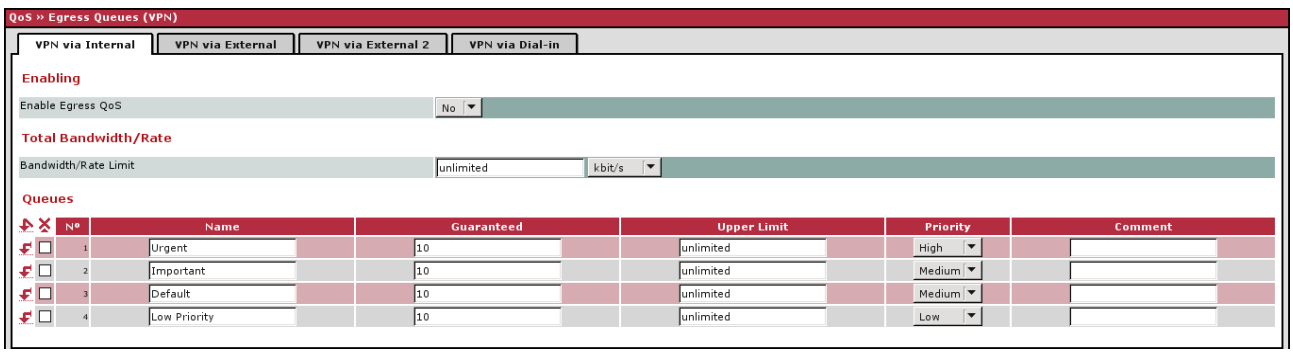
Dial-in: Settings for egress queues for packets for a PPP dial-up line connection (dial-in)



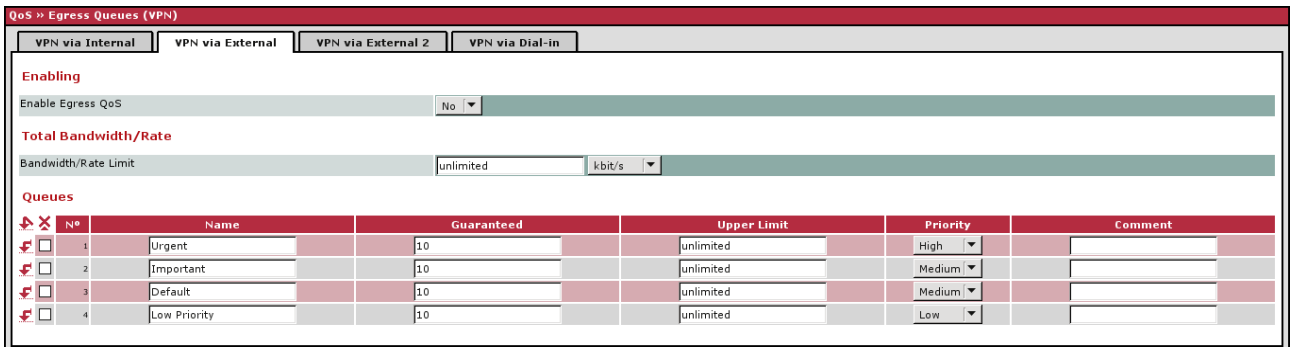
6.10.3 Egress Queues (VPN)

6.10.3.1 VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in

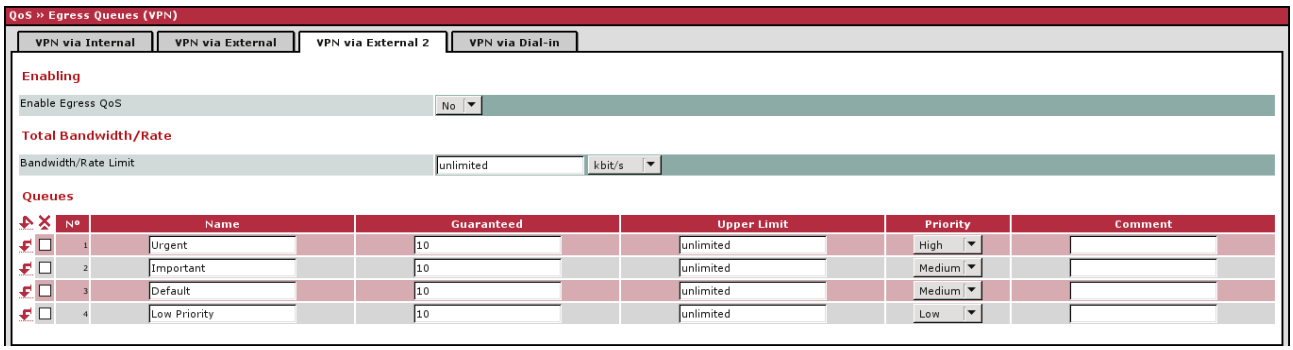
VPN via Internal: Settings for egress queues



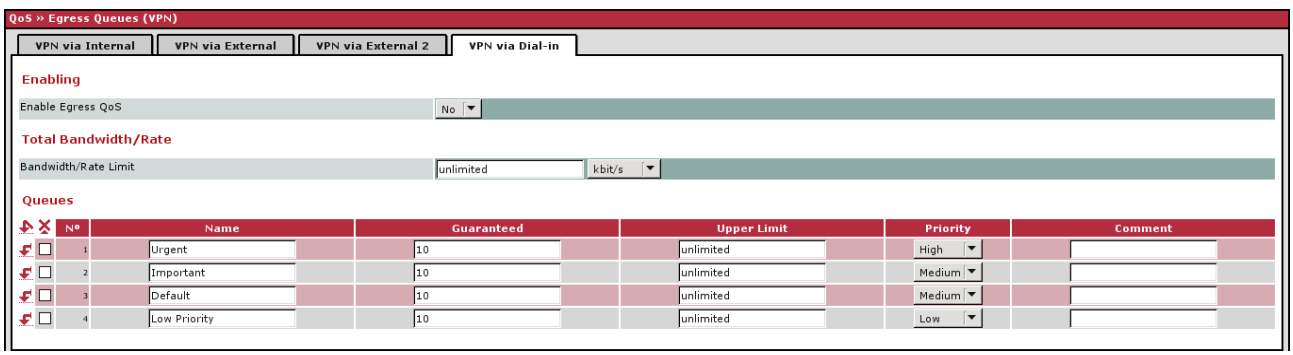
VPN via External: Settings for egress queues



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 >> Egress Queues >> Internal/External/External 2/Dial-inQoS >> 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. To be specified based on the selection under **Bandwidth/Rate Limit** (**kbit/s** OR **Packet/s**), but 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.
	Upper Limit	Maximum bandwidth available that may be set for the relevant queue by the system. To be specified based on the selection under **Bandwidth/Rate Limit** (**kbit/s** OR **Packet/s**), but 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.

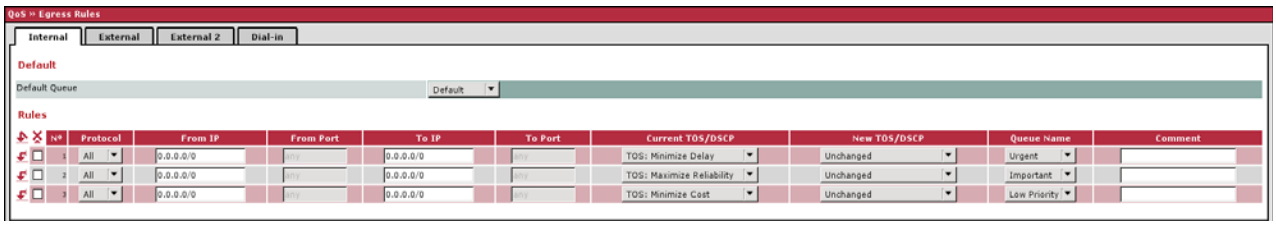
6.10.4 Egress Rules

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.

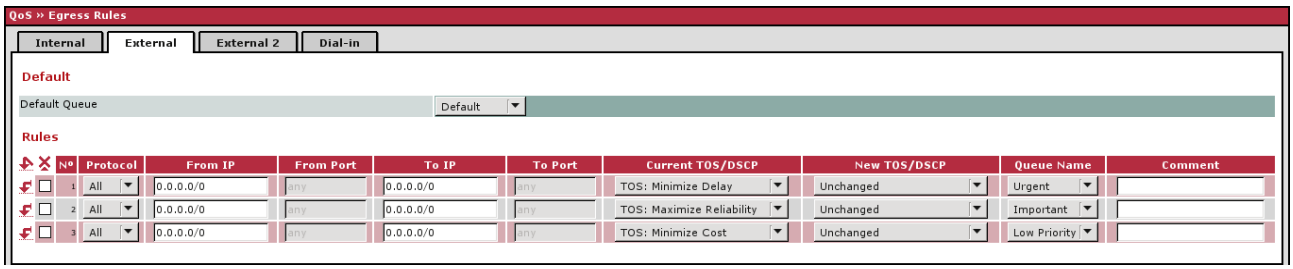
Rules can be defined separately for all interfaces and for VPN connections.

6.10.4.1 Internal/External/External 2/Dial-in

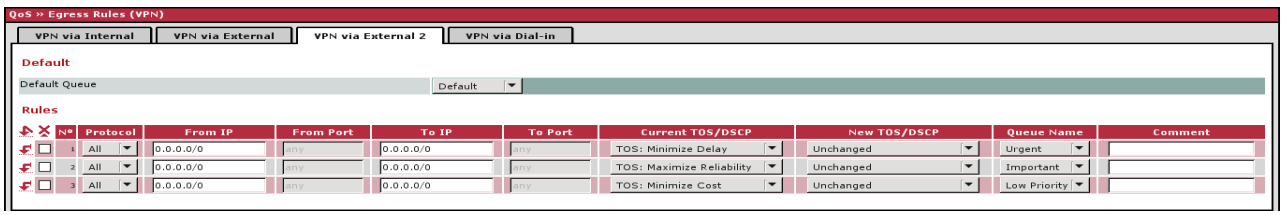
Internal: Settings for egress queue rules



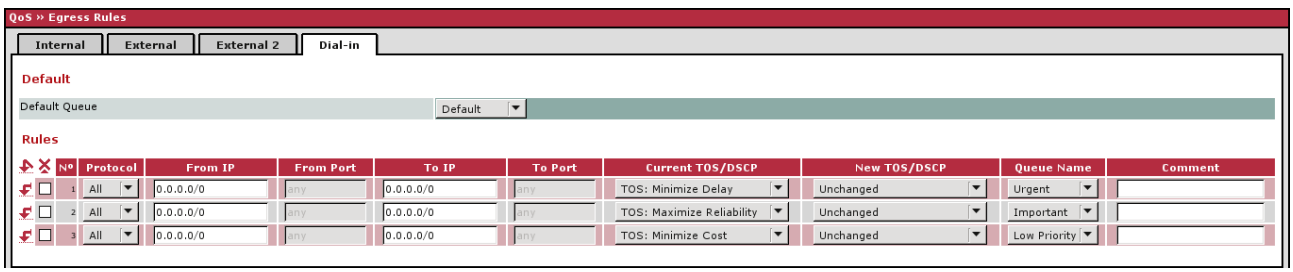
External: Settings for egress queue rules



External 2: Settings for egress queue rules



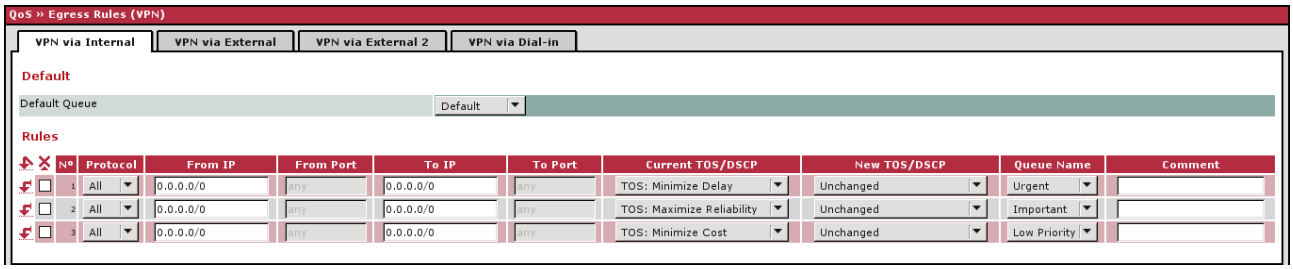
Dial-in: Settings for egress queue rules



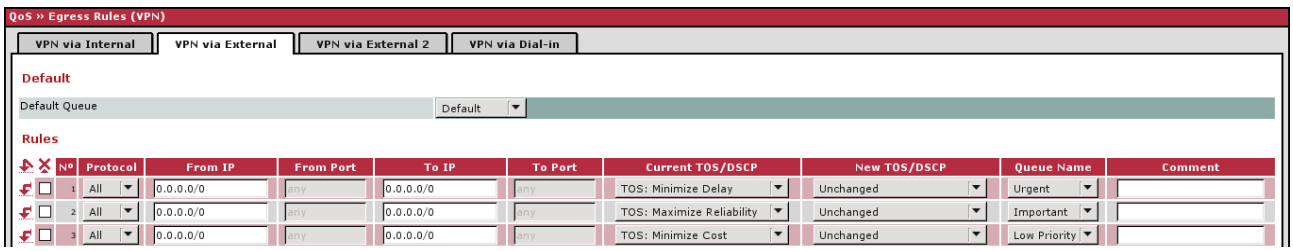
6.10.4.2 Egress Rules (VPN)

VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in

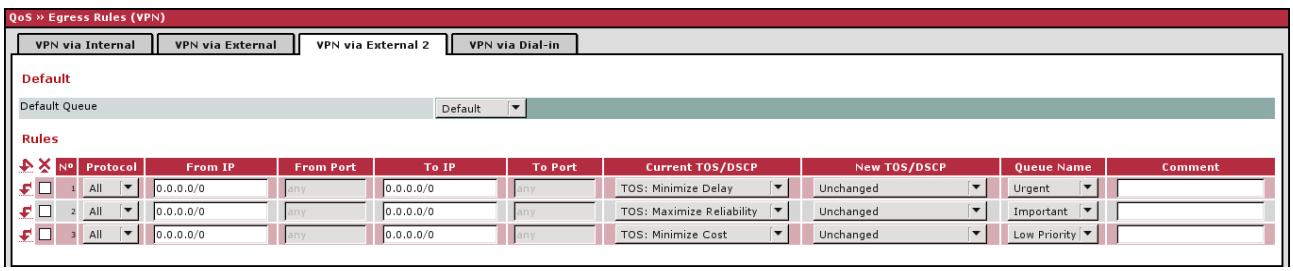
VPN via Internal: Settings for egress queue rules



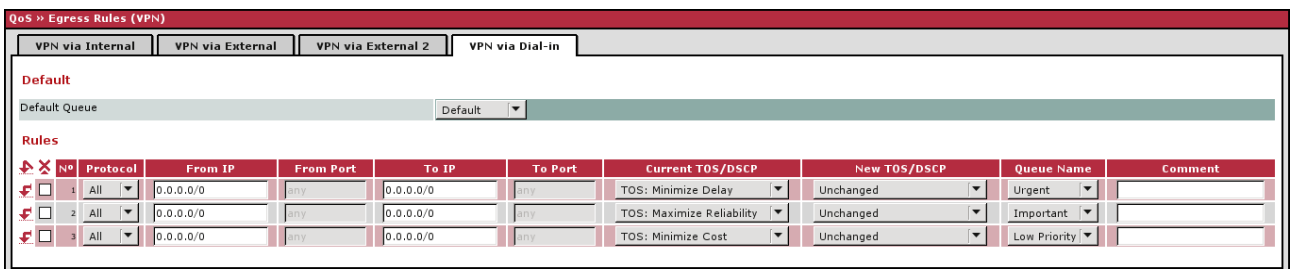
VPN via External: Settings for egress queue rules



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 >> Egress Rules >> Internal/External/External 2/Dial-in
QoS >> 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 6-203) under the name *Urgent*. Define the rules 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 assignment.
	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 6-220) 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 >> Egress Rules >> Internal/External/External 2/Dial-in
QoS >> Egress Rules (VPN) >> VPN via Internal/VPN via External/VPN via External 2/VPN via Dial-in (Fortsetzung)

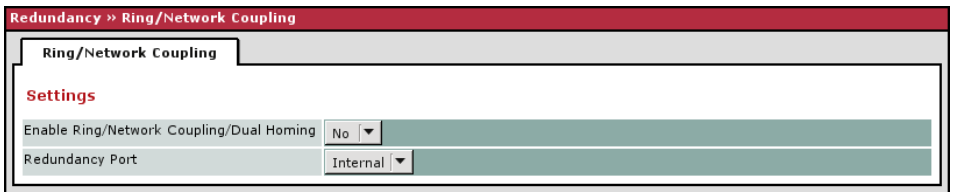
Current TOS/DSCP	Each data packet contains a TOS or DSCP field. (TOS stands for Type of Service, DSCP stands for Differentiated Services Code Point). The traffic type to which the data packet belongs is specified here. For example, an IP phone will write a different entry in this field for outgoing data 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.

6.11 Redundancy menu

Ring/network coupling with restrictions:
– FL MGUARD DELTA: The internal side (switch ports) cannot be switched off
– FL MGUARD PCI: In driver mode, the internal network interface cannot be switched off (however, this is possible in power-over-PCI mode)

6.11.1 Ring/Network Coupling

6.11.1.1 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/arrives on the LAN port, the WAN port is also disabled/enabled. **External**: If the connection is lost/arrives on the WAN port, the LAN port is also disabled/enabled.

6.12 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.

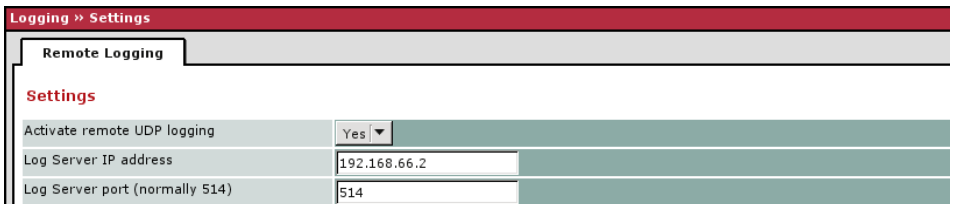
Log entries are recorded in various categories and can be displayed according to these categories (see “Logging >> Browse local logs” on page 6-213).

6.12.1 Logging >> Settings

6.12.1.1 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 all log entries should be transmitted to the external log server (specified below), set this option to **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

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 6-172).

Logging >> Remote Logging (Fortsetzung)

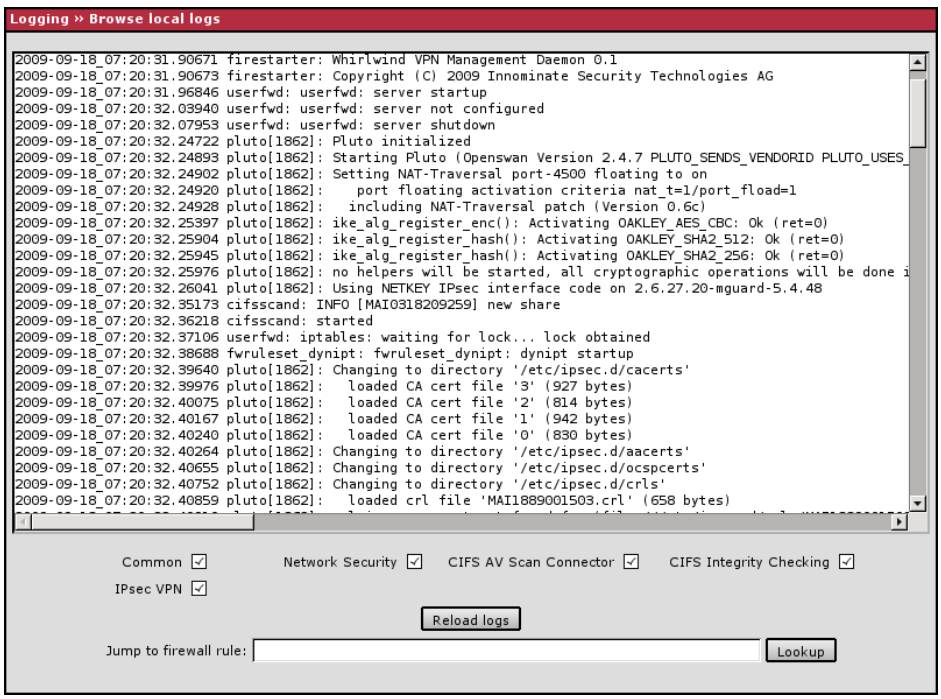
– If the **Enable 1-to-1 NAT of the local network to an internal network** option is set to **Yes** (see “1:1 NAT” on page 6-180), the following applies:

  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 6-180), 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.

6.12.2 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**.

6.12.2.1 Log entry categories

Common

Log entries that cannot be assigned to other categories.

Network Security

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

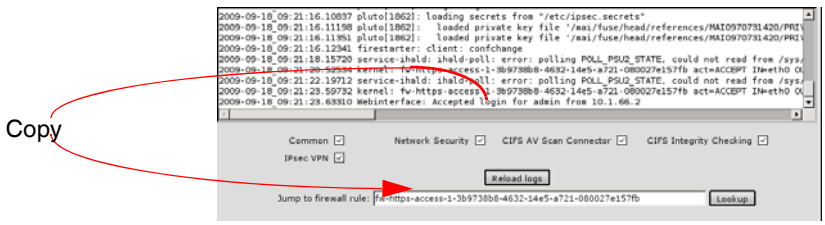
– Packet filters:
  Network Security >> Packet Filter >> Incoming Rules menu
  Network Security >> Packet Filter >> Outgoing Rules menu
  Log ID: **fw-incoming** bzw. **fw-outgoing**
– Firewall rules for VPN connections:
  IPsec VPN >> Connections >> Edit >> Firewall menu, Incoming/Outgoing
  Log ID: **vpn-fw-in** bzw. **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 >> 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 that 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.

Blade

In addition to error messages, the following messages are output on the FL MGUARD BLADE controller:

The areas enclosed by < and > are replaced by the relevant data in the log entries.

General messages:

```
BLADE daemon "<version>" starting ...
Blade[<BLADEnr>] online
Blade[<BLADEnr>] is mute
Blade[<BLADEnr>] not running
Reading timestamp from BLADE[<BLADEnr>]
```

When activating a configuration profile on a blade:

```
Push configuration to BLADE[<BLADEnr>]
reconfiguration of BLADE[<BLADEnr>] returned <returncode>
BLADE[<BLADEnr>] # <text>
```

When retrieving a configuration profile from a blade:

```
Pull configuration from BLADE[<BLADEnr>]
Pull configuration from BLADE[<BLADEnr>] returned <returncode>
```

CIFS AV Scan Connector

In this log, CIFS server messages are displayed which are operated by the FL MGUARD for the enabling process.
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.

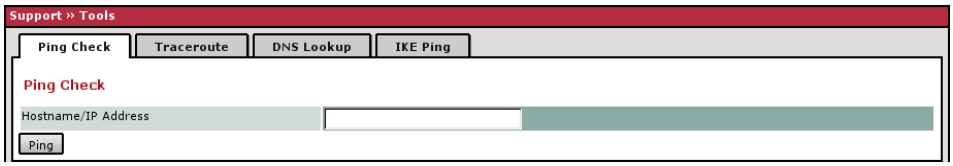
The format corresponds to standard Linux format.

There are special evaluation programs that present information from the logged data in a better readable format.

6.13 Support menu

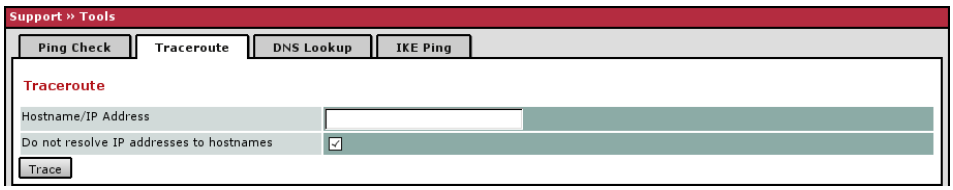
6.13.1 Support >> Tools

6.13.1.1 Ping Check



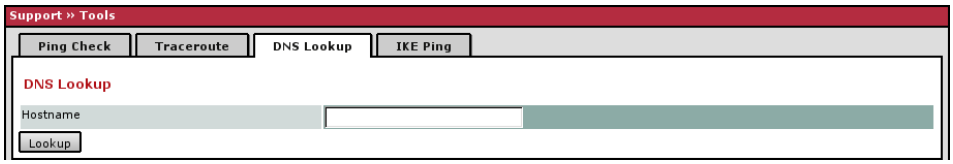
Support >> Tools >> Ping Check	
Ping Check	**Aim**: To check whether the remote peer can be accessed via a network. **How to proceed**: • Enter the IP address or host name of the remote peer in the **Hostname/IP Address** field. Then click on **Ping**. A corresponding message is then displayed.

6.13.1.2 Traceroute



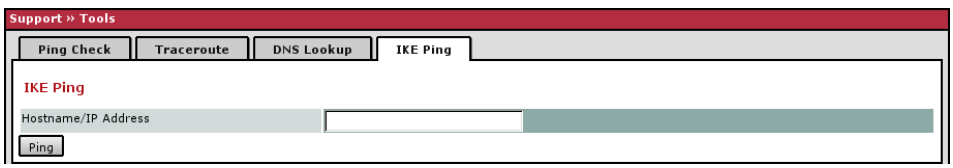
Support >> Tools >> Traceroute	
Traceroute	**Aim**: To determine which intermediate points or routers are located on the connection path to a remote peer. **How to proceed**: • Enter the host name or IP address of the remote peer whose route is to be determined in the **Hostname/IP Address** field. • 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.

6.13.1.3 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. **How to proceed**: • 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.

6.13.1.4 IKE Ping

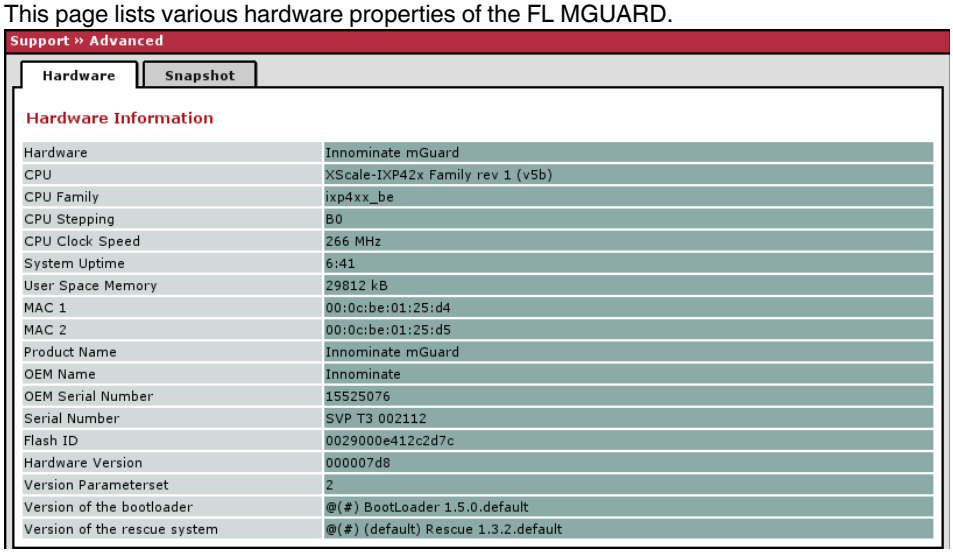


Support >> Tools >> IKE Ping	
IKE Ping	**Aim**: To determine whether the VPN software for a VPN gateway is able to establish a VPN connection, or whether a firewall prevents this, for example. **How to proceed**: • Enter the name or IP address of the VPN gateway in the **Hostname/IP Address** field. • Click on **Ping**. • A corresponding message is then displayed.

6.13.2 Support >> Advanced

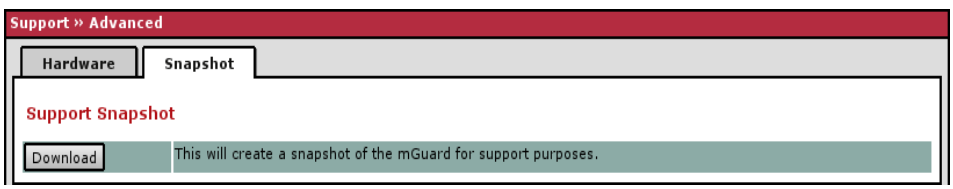
6.13.2.1 Hardware

This page lists various hardware properties of the FL MGUARD.



6.13.2.2 Snapshot

This function is used for support purposes.



It creates a compressed file (in tar.gz format) containing all current configuration settings and log entries that could be relevant for error diagnostics.

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, if required.

6.14 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.

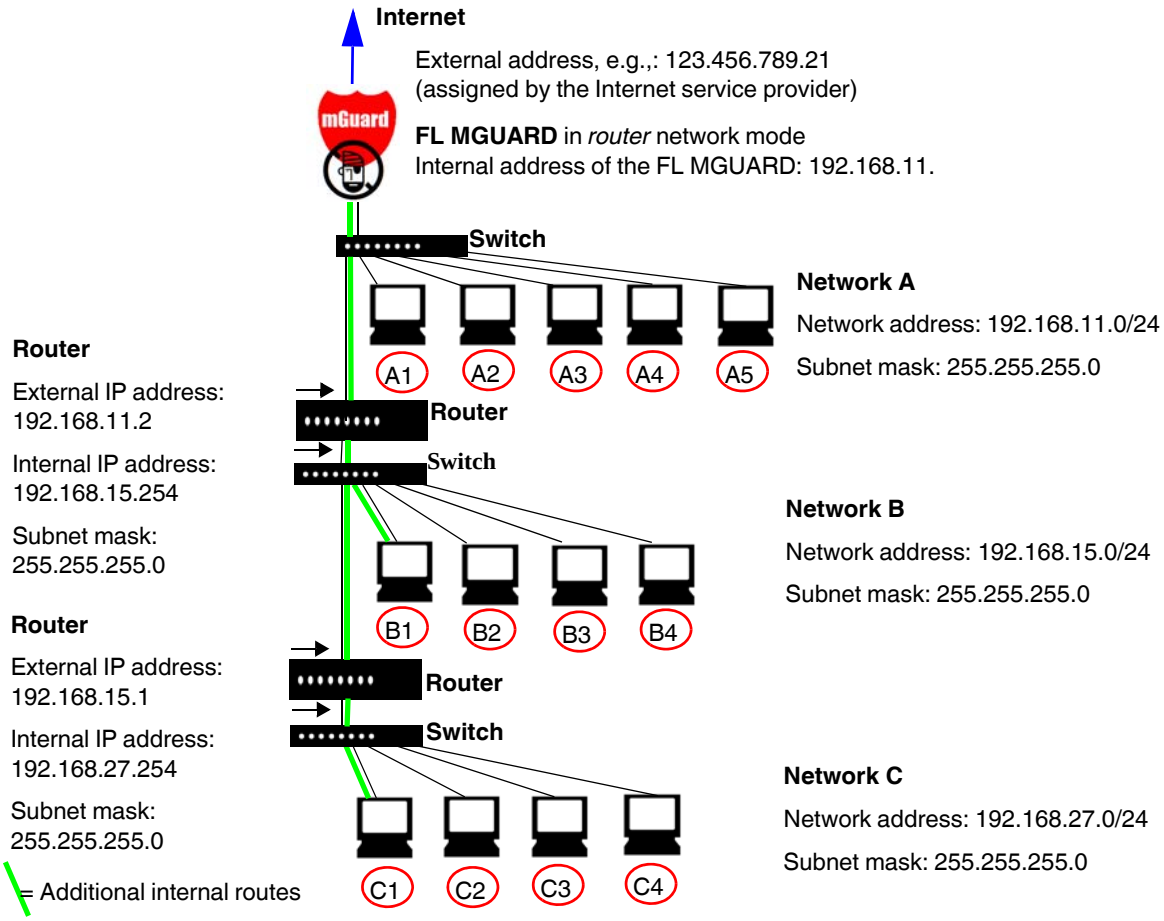
To specify an area of IP addresses for the FL MGUARD, e.g., when configuring the firewall, it may be necessary to specify the address area in CIDR format. In the table below, the left-hand column shows the IP subnet mask, while the right-hand column shows the corresponding CIDR format.

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
0.0.0.0	00000000 00000000 00000000 00000000	0

Example: 192.168.1.0 / 255.255.255.0 corresponds to CIDR: 192.168.1.0/24

6.15 Network example diagram

The following diagram shows how IP addresses can be distributed in a local network with subnetworks, which network addresses result, and how the details regarding additional internal routes may look for the FL MGUARD.



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
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	Gateway: 192.168.11.2
Network C	**Computer**	**C1**	**C2**	**C3**	**C4**	Network: 192.168.27.0/24
	IP address	192.168.27.1	**192.168.27.2**	**192.168.27.3**	**192.168.27.4**	Gateway: 192.168.11.2
	Subnet mask	255.255.255.0	**255.255.255.0**	**255.255.255.0**	**255.255.255.0**	

7 Restart, recovery procedure, and flashing the firmware

The Rescue button is used to perform the following procedures on the devices shown in 7-1:

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

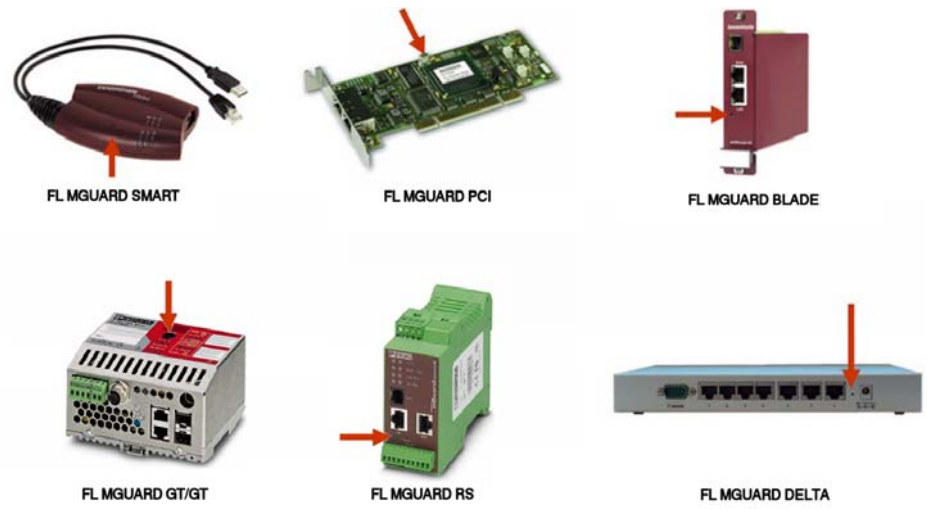


Figure 7-1 Rescue button

7.1 Performing a restart

Aim

The device is restarted with the configured settings.

Action

Press the Rescue button on the other FL MGUARD devices for around 1.5 seconds:

- **FL MGUARD RS …** : Until the "Error" LED lights up
- **FL MGUARD GT/GT …** : Until the "Error" LED lights up
- **FL MGUARD SMART2**: Until the middle LED lights up red
- **FL MGUARD BLADE, FL MGUARD PCI**: Until both red LEDs light up red
- **FL MGUARD DELTA**: Until the status LED stops flashing

Alternatively:

- Temporarily disconnect the power supply.
- **FL MGUARD PCI**: Restart the computer that contains the FL MGUARD PCI 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 RS …	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD SMART 2	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD PCI	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD BLADE	Stealth	https://1.1.1.1/	https://192.168.1.1/
	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD GT/GT …	Router		https://192.168.1.1/
FL MGUARD BLADE controller	Router		https://192.168.1.1/
FL MGUARD DELTA	Router		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, as this only works when the management IP is active.
– MAU management remains 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.

Action

FL MGUARD RS … , FL MGUARD SMART2, FL MGUARD BLADE, FL MGUARD PCI, FL MGUARD GT/GT ..., FL MGUARD DELTA:

• Slowly press the **Rescue button** six times.
The FL MGUARD responds after around two seconds:

FL MGUARD RS ..., FL MGUARD GT/GT ...	The "State" LED lights up green.
FL MGUARD SMART2	The middle LED lights up green.
FL MGUARD BLADE, FL MGUARD PCI	The LAN LED lights up red.
FL MGUARD DELTA	The status LED lights up green.

- Press the **Rescue button** slowly again six times.

FL MGUARD RS ..., **FL MGUARD GT/GT ...**	If successful, the "State" LED lights up green. If unsuccessful, the "Error" LED lights up red.
FL MGUARD SMART2	If successful, the middle LED lights up green. If unsuccessful, the middle LED lights up red.
FL MGUARD BLADE, **FL MGUARD PCI**	If successful, the LAN LED lights up red. If unsuccessful, the WAN LED lights up red.
FL MGUARD DELTA	If successful, the status LED lights up green. If unsuccessful, the status LED stays off.

- If successful, the device restarts after two seconds and switches to *stealth* or *router* mode. The device can then be addressed again at the corresponding address, see Table “Preset addresses” on page 7-2.

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.
– For the FL MGUARD RS ..., only firmware Version 5.1.0 or later can be installed.

Possible reasons:

– The administrator and root password have been lost.

Requirements

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 7-6).

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

Additional requirements:

– The FL MGUARD firmware has been obtained from the Innominate Support team or from www.phoenixcontact.com and has been saved on the configuration computer.
– If your current firmware version is newer than the version by default upon delivery, a license must be obtained for using this update. This applies to major release upgrades, e.g., from Version 4.x.y to Version 5.x.y to Version 6.x.y, etc.
– DHCP and TFTP servers can be accessed under the same IP address.

– **FL MGUARD PCI**: If the FL MGUARD is operated in **power-over-PCI mode**, the DHCP/TFTP server must be connected via the LAN female connector of the FL MGUARD.
– **FL MGUARD PCI**: If the FL MGUARD is operated in PCI **driver mode**, the DHCP/TFTP server must be operated on the computer or operating system that provides the interface for the FL MGUARD.

Action

For the FL MGUARD SMART 2, FL MGUARD PCI, FL MGUARD BLADE, FL MGUARD DELTA, FL MGUARD RS ...:

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. The device could be damaged and may have to be reactivated by the manufacturer.

For more detailed instructions for performing the rescue procedure on the **FL MGUARD GT/GT ...**, please refer to Section “Using Smart mode” on page 3-5.

- 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 RS …	The "State", "LAN", and "WAN" LEDs light up green.
FL MGUARD SMART2	The LEDs light up green.
FL MGUARD BLADE, FL MGUARD PCI	The green LEDs and the red "LAN" LED light up.
FL MGUARD DELTA	The status LED fades slowly.

- **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 RS …	The "State" LED flashes.
FL MGUARD SMART2	The middle LED ("Heartbeat") flashes.
FL MGUARD BLADE, FL MGUARD PCI	The red "LAN" LED flashes.
FL MGUARD DELTA	The status LED flashes.

  The "install.p7s" file is loaded from the TFTP server. 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 RS … **FL MGUARD GT/GT...**	The "Modem", "State", and "LAN" LEDs form a light sequence.
FL MGUARD SMART2	The three green LEDs form a light sequence.
FL MGUARD BLADE, **FL MGUARD PCI**	The green LEDs and the red LAN LED form a light sequence.
FL MGUARD DELTA	The status LED flashes faster.

The "jffs2.img.p7s" firmware file is downloaded from the TFTP server 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 approximately 3 to 5 minutes.

The reaction of the device depends on its type:

FL MGUARD RS … **FL MGUARD GT/GT...**	The "State" LED is lit continuously.
FL MGUARD SMART2	The middle LED ("Heartbeat") is lit continuously.
FL MGUARD BLADE, **FL MGUARD PCI**	The green LEDs flash, while the red "LAN" LED is lit continuously.
FL MGUARD DELTA	The status LED is lit continuously.

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

As soon as the procedure has been completed, the following occurs:

FL MGUARD RS … **FL MGUARD GT/GT...**	The "Modem", "State", and "LAN" LEDs flash green simultaneously.
FL MGUARD SMART2	All 3 LEDs flash green simultaneously.
FL MGUARD BLADE	The green "WAN", green "LAN", and red "WAN" LEDs flash simultaneously.
FL MGUARD PCI	The FL MGUARD restarts.
FL MGUARD DELTA	The status LED flashes once per second.

- Restart the FL MGUARD. This is not necessary for the FL MGUARD BLADE and FL MGUARD PCI.
- 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 power supply.)

The FL MGUARD is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 5-13):

7.3.1 Installing the DHCP and TFTP server

NOTE: 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 www.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 means of 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 6-32).

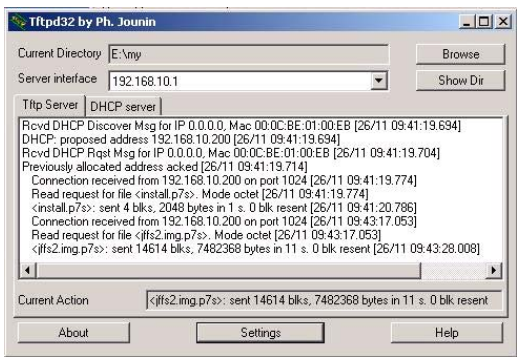
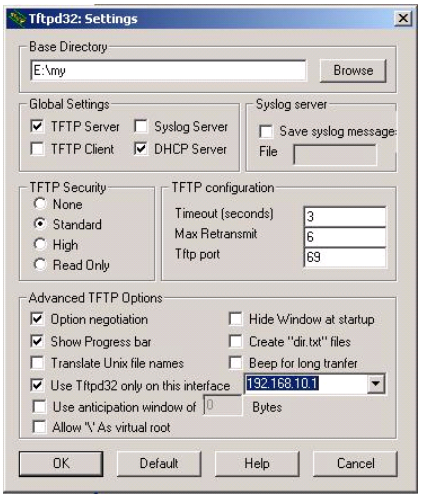


Figure 7-2 Entering the host IP

- Switch to the "Tftp Server" or "DHCP server" tab page and click on "Settings" to set the parameters as follows:



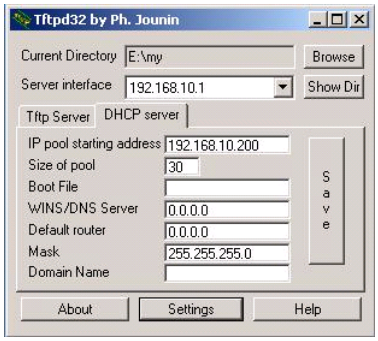


Figure 7-3 Settings

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 means of 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 6-32).
- 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 Glossary

Asymmetrical encryption

In asymmetrical encryption, data is encrypted with one key and decrypted with a second key. Both keys are suitable for encryption and decryption. One of the keys is kept secret by its owner (private key), while the other is made available to the public (public key), i.e., to potential communication partners.

A message encrypted with the public key can only be decrypted and read by the owner of the associated private key. A message encrypted with the private key can be decrypted by any recipient in possession of the associated public key. Encryption using the private key shows that the message actually originated from the owner of the associated public key. Therefore, the expression "digital signature" is also often used.

However, asymmetrical encryption methods such as RSA are both slow and susceptible to certain types of attack. As a result, they are often combined with some form of symmetrical encryption (→ “Symmetrical encryption” on page 8-8). On the other hand, concepts are available enabling the complex additional administration of symmetrical keys to be avoided.

DES/3DES

This symmetrical encryption algorithm (→ “Symmetrical encryption” on page 8-8) was developed by IBM and checked by the NSA. DES was specified in 1977 by the American National Bureau of Standards (the predecessor of the National Institute of Standards and Technology (NIST)) as the standard for American governmental institutions. As this was the very first standardized encryption algorithm, it quickly won acceptance in industrial circles, both inside and outside America.

DES uses a 56-bit key length, which is no longer considered secure as the available processing power of computers has greatly increased since 1977.

3DES is a variant of DES. It uses keys that are three times as long, i.e., 168 bits in length. Still considered to be secure today, 3DES is included in the IPsec standard, for example.

AES

AES (Advanced Encryption Standard) has been developed by NIST (National Institute of Standards and Technology) in cooperation with the industry. This symmetrical encryption standard has been developed to replace the earlier DES standard. AES specifies three different key lengths (128, 192, and 256 bits).

In 1997, NIST started the AES initiative and published its conditions for the algorithm. From the many proposed encryption algorithms, NIST selected a total of five algorithms for closer examination – MARS, RC6, Rijndael, Serpent, and Twofish. In October 2000, the Rijndael algorithm was adopted as the encryption algorithm.

CA certificate

How trustworthy is a CA certificate and the issuing CA (certification authority)? (→ “X.509 certificate” on page 8-7) A CA certificate can be consulted in order to check a certificate bearing this CA's signature. This check only makes sense if there is little doubt that the CA certificate originates from an authentic source (i.e., is authentic). In the event of doubt, the CA certificate itself can be checked. If (as is usually the case) the certificate is a sub-CA certificate (i.e., a CA certificate issued by a sub-certification authority), then the CA certificate of the superordinate CA can be used to check the CA certificate of the subordinate instance. If a superordinate CA certificate is in turn subordinate to another superordinate CA, then its CA certificate can be used to check the CA certificate of the subordinate instance, etc. This "chain of trust" continues down to the root instance (the root CA or certification authority). The root CA's CA file is necessarily self-signed, since this instance is the highest available, and is ultimately the basis of trust. No-one else can certify that this instance is actually the instance in question. A root CA therefore is a state or a state-controlled organization.

The FL MGUARD can use its imported CA certificates to check the validity of certificates shown by remote peers. In the case of VPN connections, for example, remote peers can only be authenticated using CA certificates. This requires that all CA certificates must be installed on the FL MGUARD in order to form a chain with the certificate shown by the remote peer. In addition to the CA certificate from the CA whose signature appears on the certificate shown by the VPN partner to be checked, this also includes the CA certificate of the superordinate CA, and so forth, up to the root certificate. The more meticulously this "chain of trust" is checked in order to authenticate a remote peer, the higher the level of security will be.

Client/server

In a client/server environment, a server is a program or computer, which accepts and responds to queries from client programs or client computers.

In data communication, the computer establishing a connection to a server (or host) is also called a client. In other words, the client is the calling computer and the server (or host) is the computer called.

Datagram

In the IP transmission protocol, data is sent in the form of data packets. These are known as IP datagrams. An IP datagram is structured as follows:

IP header	TCP, UDP, ESP, etc. header	Data (payload)

The IP header contains:

– The IP address of the sender (source IP address)
– The IP address of the recipient (destination IP address)
– The protocol number of the protocol on the superordinate protocol layer (according to the OSI layer model)
– The IP header checksum used to check the integrity of the received header

The TCP/UDP header contains the following information:

– The sender's port (source port)
– The port of the recipient (destination port)
– A checksum covering the TCP header and information from the IP header (e.g., source and destination IP addresses)

Default route

If a computer is connected to a network, the operating system creates a routing table internally. The table lists the IP addresses that the operating system has identified based on the connected computers and the routes available at that time. Accordingly, the routing table contains the possible routes (destinations) for sending IP packets. If IP packets are to be sent, the computer's operating system compares the IP addresses stated in the IP packets with the entries in the routing table in order to determine the correct route.

If a router is connected to the computer and its internal IP address (i.e., the IP address of the router's LAN port) has been relayed to the operating system as the default gateway (in the network card's TCP/IP configuration), then this IP address is used as the destination if all other IP addresses in the routing table are not suitable. In this case the IP address of the router specifies the default route, because all IP packets whose IP address has no counterpart in the routing table (i.e., cannot find a route) are directed to this gateway.

DynDNS provider

Also known as *Dynamic DNS provider*. Every computer connected to the Internet has an IP address (IP = Internet Protocol). If the computer accesses the Internet via a dial-up modem, ISDN or ADSL, its Internet service provider will assign it a dynamic IP address. In other words, the address changes for each online session. Even if a computer is online 24 hours a day without interruption (e.g., flat-rate), the IP address will change during the session.

If this computer needs to be accessible via the Internet, it must have an address that is known to the remote peer. This is the only way to establish a connection to the computer. However, if the address of the computer changes constantly, this will not be possible. This problem can be avoided if the operator of the computer has an account with a Dynamic DNS provider (DNS = Domain Name Server).

In this case, the operator can set a host name with this provider via which the system should be accessible, e.g., www.example.com. The Dynamic DNS provider also provides a small program that must be installed and run on the computer concerned. Every time a new Internet session is launched on the local computer, this tool sends the IP address used by the computer to the Dynamic DNS provider. The domain name server registers the current assignment of the host name to the IP address and also informs the other domain name servers on the Internet accordingly.

If a remote computer now wishes to establish a connection to a computer that is registered with the DynDNS provider, then the remote computer can use the host name of the computer as its address. This will establish a connection to the responsible DNS in order to look up the IP address that is currently registered for this host name. The corresponding IP address is sent back from the DNS to the remote computer, which can then use it as the destination address. This now leads directly to the desired computer.

In principle, all Internet addresses are based on this procedure: First, a connection to a DNS is established in order to determine the IP address assigned to the host name. Once this has been accomplished, the established IP address is used to set up a connection to the required remote peer, which could be any site on the Internet.

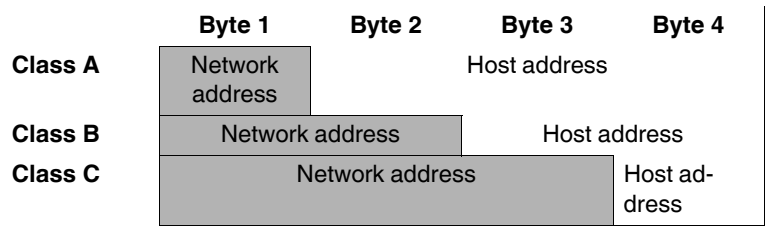
IP address

Every host or router on the Internet/Intranet has its own IP address (IP = Internet Protocol). An IP address is 32 bits (4 bytes) long and is written as four numbers (each between 0 and 255), which are separated by a dot.

An IP address consists of two parts: the network address and the host address.

Network address	Host address

All network hosts have the same network address, but different host addresses. The two parts of the address differ in length depending on the size of the respective network (networks are categorized as Class A, B or C).



The first byte of the IP address determines whether the IP address of a network device belongs to Class A, B or C. The following is specified:

	Value of byte 1	Bytes for the network address	Bytes for the host address
Class A	1 - 126	1	3
Class B	128 - 191	2	2
Class C	192 - 223	3	1

Based on the above figures, the number of Class A networks worldwide is limited to 126. Each of these networks can have a maximum of 256 x 256 x 256 hosts (3 bytes of address area). There can be 64 x 256 Class B networks and each of these networks can have up to 65,536 hosts (2 bytes of address area: 256 x 256). There can be 32 x 256 x 256 Class C networks and each of these networks can have up to 256 hosts (1 byte of address area).

Subnet mask

Normally, a company network with access to the Internet is only officially assigned a single IP address, e.g., 123.456.789.21. The first byte of this example address indicates that this company network is a Class B network; in other words, the last 2 bytes are free to be used for host addresses. Accordingly, an address area for up to 65,536 possible hosts (256 x 256) can be computed.

Such a huge network is not practical, and generates a need for subnetworks to be built. The subnet mask can be used for this purpose. Like an IP address, the mask is 4 bytes long. The bytes representing the network address are each assigned the value 255. The primary purpose of doing this is to enable a portion of the host address area to be "borrowed" and used for addressing subnetworks. For example, if the subnet mask 255.255.255.0 is used on a Class B network (2 bytes for the network address, 2 bytes for the host address), the third byte, which was actually intended for host addressing, can now be used for subnetwork addressing. This computes to potential support for 256 subnetworks each with 256 hosts.

IPsec

IP security (IPsec) is a standard that uses encryption to verify the authenticity of the sender and to ensure the confidentiality and integrity of the data in IP datagrams (→ “Datagram” on page 8-2). The components of IPsec are the Authentication Header (AH), the Encapsulating Security Payload (ESP), the Security Association (SA), and the Internet Key Exchange (IKE).

At the start of the session, the systems involved in the communication must determine which technique to use and the implications of this choice, e.g., *Transport Mode* or *Tunnel Mode*.

In *Transport Mode*, an IPsec header is inserted between the IP header and the TCP or UDP header respectively in each IP datagram. Since the IP header remains unchanged, this mode is only suitable for host-to-host connections.

In *Tunnel Mode*, an IPsec header and a new IP header are prefixed to the entire IP datagram. This means the original datagram is encrypted in its entirety and stored in the payload of the new datagram.

Tunnel mode is used in VPN applications: The devices at the ends of the tunnel ensure that the datagrams are encrypted and decrypted; in other words, the actual datagrams are completely protected on the tunnel path, i.e., during transfer over a public network.

Subject, certificate

In a certificate, the classification of a certificate to its owner is confirmed by a certification authority (CA). This takes the form of the confirmation of specific owner characteristics. Furthermore, the certificate owner must possess the private key that matches the public key in the certificate. (→ "X.509 certificate" on page 8-7).

Example

```
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 1 (0x1)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=XY, ST=Austria, L=Graz, O=TrustMe Ltd, OU=Certificate Authority, CN=CA/Email=ca@trustme.dom
    Validity
      Not Before: Oct 29 17:39:10 2000 GMT
→   Subject: CN=anywhere.com,E=doctrans.de,C=DE,ST=Hamburg,L=Hamburg,O=Innominate,OU=Security
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1024 bit)
        Modulus (1024 bit):
          00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
          d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
          9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
          90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
          1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
          7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
          50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
          8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
          f0:b4:95:f5:f9:34:9f:f8:43
        Exponent: 65537 (0x10001)
    X509v3 extensions:
      X509v3 Subject Alternative Name:
        email:xyz@anywhere.com
      Netscape Comment:
        mod_ssl generated test server certificate
      Netscape Cert Type:
        SSL Server
  Signature Algorithm: md5WithRSAEncryption
    12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
    3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
    82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
    cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
    4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
    d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
    44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
    ff:8e
```

The *subject distinguished name* or *subject* for short clearly identifies the certificate owner. The entry consists of several components. These are known as attributes (see the example certificate above). The following table contains a list of possible attributes. The sequence of attributes in an X.509 certificate can vary.

Table 8-1 X.509 Certificate

Abbreviation	Name	Explanation
CN	Common name	Identifies the person or object to whom or which the certificate belongs. Example: CN=server1
E	E-mail address	Specifies the e-mail address of the certificate owner.
OU	Organizational unit	Specifies the department within an organization or company. Example: O=Development
O	Organization	Specifies the organization or company. Example: O=Innominate

Table 8-1 X.509 Certificate

Abbreviation	Name	Explanation
L	Locality	Specifies the place/locality. Example: L=Hamburg
ST	State	Specifies the state or county. Example: ST=Bavaria
C	Country	Two-letter code that specifies the country (Germany = DE). Example: C=DE

A filter can be set for the subject (i.e., the certificate owner) during VPN connections and remote service access to the FL MGUARD using SSH or HTTPS. This would ensure that only certificates from remote peers are accepted that have certain attributes in the subject line.

NAT (Network Address Translation)

Network Address Translation (NAT) (also known as *IP masquerading*) "hides" an entire network behind a single device, known as a NAT router. If you communicate externally via a NAT router, the internal computers in the local network and their IP addresses remain hidden. The remote communication partner will only see the NAT router with its IP address.

In order to allow internal computers to communicate directly with external computers (on the Internet), the NAT router must modify the IP datagrams that are sent from internal computers to remote peers and received by internal computers from remote peers.

If an IP datagram is sent from the internal network to a remote peer, the NAT router will modify the UDP and TCP headers of the datagram, replacing the source IP address and source port with its own official IP address and a previously unused port. For this purpose the NAT router uses a table in which the original values are listed together with the corresponding new ones.

When a response datagram is received, the NAT router uses the specified destination port to recognize that the datagram is intended for an internal computer. Using the table, the NAT router will replace the destination IP address and port before forwarding the datagram via the internal network.

Port number

A port number is assigned to each participant in UDP and TCP protocol-based communication. This number makes it possible to differentiate multiple UDP or TCP connections between two computers and use them simultaneously.

Certain port numbers are reserved for specific purposes. For example, HTTP connections are usually assigned to TCP port 80 and POP3 connections to TCP port 110.

Proxy

A proxy is an intermediary service. A web proxy (e.g., Squid) is often connected upstream of a large network. For example, if 100 employees access a certain website at the same time over a web proxy, then the proxy only loads the relevant web pages once from the server and then distributes them as needed amongst the employees. Remote web traffic is reduced, which saves money.

PPPoE

Acronym for **P**oint-to-**P**oint **P**rotocol **o**ver **E**thernet. A protocol based on the PPP and Ethernet standards. PPPoE is a specification defining how to connect users to the Internet via Ethernet using a shared broadband medium such as DSL, wireless LAN or a cable modem.

PPTP

Acronym for **P**oint-to-**P**oint **T**unneling **P**rotocol. This protocol was developed by Microsoft and U.S. Robotics, among others, for secure data transfer between two VPN nodes (→ VPN) via a public network.

Router

A router is a device that is connected to different IP networks and communicates between them. To do this, the router has an interface for each network connected to it. A router must find the correct path to the destination for incoming data and define the appropriate interface for forwarding it. To do this, it takes data from a local routing table listing assignments between available networks and router connections (or intermediary stations).

Trap

SNMP (Simple Network Management Protocol) is often used alongside other protocols, in particular on large networks. This UDP-based protocol is used for the central administration of network devices. For example, the configuration of a device can be requested using the GET command and changed using the SET command; the requested network device must simply be SNMP-compatible.

An SNMP-compatible device can also send SNMP messages (e.g., should unexpected events occur). Messages of this type are known as SNMP traps.

X.509 certificate

A type of "seal" that certifies the authenticity of a public key (→ Asymmetrical encryption) and the associated data.

It is possible to use certification to enable the user of the public key (used to encrypt the data) to ensure that the received public key is from its actual issuer (and thus from the instance that should later receive the data). A *certification authority* (CA) certifies the authenticity of the public key and the associated link between the identity of the issuer and its key. The certification authority verifies authenticity in accordance with its rules (for example, it may require the issuer of the public key to appear before it in person). Once successfully authenticated, the CA adds its (digital) signature to the issuer's public key. This results in a certificate.

An X.509(v3) certificate thus comprises a public key, information about the key owner (the Distinguished Name (DN)), authorized use, etc., and the signature of the CA (→ Subject, certificate).

The signature is created as follows: The CA creates an individual bit sequence from the bit sequence of the public key, owner information, and other data. This sequence can be up to 160 bits in length and is known as the HASH value. It then encrypts this with its own private key and then adds it to the certificate. The encryption with the CA's private key proves the authenticity of the certificate (i.e., the encrypted HASH string is the CA's digital signature). If the certificate data is tampered with, then this HASH value will no longer be correct and the certificate will be rendered worthless.

The HASH value is also known as the fingerprint. Since it is encrypted with the CA's private key, anyone who has the corresponding public key can decrypt the bit sequence and thus verify the authenticity of the fingerprint or signature.

The involvement of a certification authority means that it is not necessary for key owners to know each other. They only need to know the certification authority involved in the process. The additional key information further simplifies administration of the key.

X.509 certificates can, for example, be used for e-mail encryption by means of S/MIME or IPsec.

Protocol, transmission protocol

Devices that communicate with each other must follow the same rules. They have to "speak the same language". Rules and standards of this kind are called protocols or transmission protocols. Some of the more frequently used protocols are IP, TCP, PPP, HTTP, and SMTP.

Service provider

Service providers are companies or institutions that enable users to access the Internet or online services.

Spoofing, anti-spoofing

In Internet terminology, spoofing means supplying a false address. Using this false Internet address, a user can create the illusion of being an authorized user.

Anti-spoofing is the term for mechanisms that detect or prevent spoofing.

Symmetrical encryption

In symmetrical encryption, the same key is used to encrypt and decrypt data. Two examples of symmetrical encryption algorithms are DES and AES. They are fast, but also increasingly difficult to administrate as the number of users increases.

TCP/IP (Transmission Control Protocol/Internet Protocol)

These are network protocols used to connect two computers on the Internet:

IP is the base protocol.

UDP is based on IP and sends individual packets. The packets may reach the recipient in an different order than that in which they were sent or they may even be lost.

TCP is used for connection security and ensures, for example, that data packets are forwarded to the application in the correct order.

UDP and TCP add port numbers between 1 and 65535 to the IP addresses. These distinguish the various services offered by the protocols.

A number of additional protocols are based on UDP and TCP. These include HTTP (Hyper Text Transfer Protocol), HTTPS (Secure Hyper Text Transfer Protocol), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol, Version 3), and DNS (Domain Name Service).

ICMP is based on IP and contains control messages.

SMTP is an e-mail protocol based on TCP.

IKE is an IPsec protocol based on UDP.

ESP is an IPsec protocol based on IP.

On a Windows PC, the WINSOCK.DLL (or WSOCK32.DLL) provides a common interface for both protocols.

(→ “Datagram” on page 8-2).

VLAN

A VLAN (Virtual Local Area Network) divides a physical network into several independent logical networks, which exist in parallel.

Devices on different VLANs can only access devices within their own VLAN. Accordingly, assignment to a VLAN is no longer defined by the network topology alone, but also by the configured VLAN ID.

VLAN settings can be used as optional settings for each IP. A VLAN is identified by its VLAN ID (1 - 4094). All devices with the same VLAN ID belong to the same VLAN and can, therefore, communicate with each other.

The Ethernet packet for a VLAN (according to IEEE 802.1Q) is extended by 4 bytes, with 12 bits available for recording the VLAN ID. VLAN IDs "0" and "4095" are reserved and cannot be used for VLAN identification.

VPN (Virtual Private Network)

A **V**irtual **P**rivate **N**etwork (VPN) connects several separate private networks (subnetworks) together via a public network (e.g., the Internet) to form a single common network. Cryptographic protocols are used to ensure confidentiality and authenticity. A VPN is therefore a cost-effective alternative to the use permanent lines for building a nationwide corporate network.

9 Technical data

9.1 FL MGUARD RS …

Hardware properties	
Platform	Intel network processor with 533 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I full duplex I auto MDIX
Other interfaces	Serial RS-232, RJ11 female connector I Optional analog modem I optional ISDN TA
Drives	–
High availability	Depending on the firmware used
Power supply	24 V DC I 170 mA I SELV I redundant I voltage range 9 V - 36 V
Power consumption	4.1 W, typical
Humidity range	10% ... 95% during operation, no condensation
Degree of protection	IP20
Temperature range	0°C ... +55°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	100 x 45 x 112 mm
Weight	250 g

Firmware and power values	
Firmware compatibility	FL MGUARD v5.0 or later; Innominate recommends firmware Version 6.x or 7.x to be used with the up-to-date patch releases; For the scope of functions, please refer tot he relevant firmware data sheet.
Data throughput (router I firewall)	up to 90 Mbps bidirectional I up to 70 Mbps bidirectional
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	up to 70 Mbps (bidirectional)
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 Icentral device management software I optional key switch (VPN)
Diagnostics	LEDs (P1, P2, Modem, Fault, State, Error, LAN, WAN) I signal contact (SELV) I service contacts (⊥, CMD, ACK) I log file I remote syslog

Other	
Conformance	CE I FCC I UL 508

9.2 FL MGUARD GT/GT …

General data	
Function	Security appliance, firewall, routing, 1:1 NAT; VPN (optional), conforms to standard IEEE 802.3/802.3u/802.3ab
Firewall principle	Stateful inspection
SNMP	Version 2c, 3
Data throughput (router | firewall)	up to 160 Mbps bidirectional | up to 160 Mbps bidirectional
Hardware-based encryption	DES | 3DES | AES-128/192/256
Encrypted VPN throughput (AES-256)	up to 70 Mbps (bidirectional)
Management support	Web GUI (HTTPS) | command line interface (SSH) | SNMP v1/2/3 |central device management software | optional key switch (VPN)
Housing dimensions (width x height x depth) in mm	128 x 110 x 69 (depth from top edge of DIN rail) 128 x 150 x 69 (depth from top edge of DIN rail) with FL MEM PLUG (accessories)
Permissible operating temperature	-20°C to 60°C
Permissible storage temperature	-40°C to +85°C
Degree of protection	IP20, IEC 60529
Class of protection	Class 3 VDE 0106; IEC 60536
Humidity	
Operation	5% to 95%, no condensation
Storage	5% to 95%, no condensation
Air pressure	
Operation	86 kPa to 108 kPa, 1500 m above sea level
Storage	66 kPa to 108 kPa, 3500 m above sea level
Ambient compatibility	Free from substances that would hinder coating with paint or varnish according to VW specification
Mounting position	Perpendicular on a standard DIN rail
Connection to protective earth ground	By snapping it on a grounded DIN rail
Weight	660 g, typical

Supply voltage (US1/US2 redundant)	
Connection	Via COMBICON; maximum conductor cross section = 2.5 mm^2 (14 AWG)
Nominal value	24 V DC
Permissible voltage range	18.0 V DC to 32.0 V DC
Permissible ripple (within the permissible voltage range)	3.6 V_{pp}
Test voltage	500 V DC for one minute
Maximum current consumption on US at 24 V DC	270 mA
Maximum power consumption at nominal voltage	6.5 W

Interfaces	
Number of Ethernet ports with Gigabit support	2, should be operated as RJ45 port or SFP port
RS-232 configuration interface	
Connection format	Mini-DIN female connector

Interfaces (Fortsetzung)

Floating signal contact	
Voltage	24 V DC
Current carrying capacity	100 mA

Ethernet interfaces

Properties of RJ45 ports	
Number	2 with auto crossing and auto negotiation
Connection format	8-pos. RJ45 female connector on the switch
Connection medium	Twisted-pair cable with a conductor cross-section of 0.14 mm^2 to 0.22 mm^2 (26 - 25 AWG)
Cable impedance	100 ohms
Transmission speed	10/100/1000 Mbps
Maximum network segment length	100 m
Properties of the SFP interfaces	
Number	2
Connection format	Gigabit SFP slot module
Connection medium	Fiber optics
Connection	LC format
Data transmission rate	1000 Mbps
Maximum network expansion	Depending on the SFP module used
Optical fiber type	Depending on the SFP module used

Mechanical tests

Shock test according to IEC 60068-2-27	Operation: 30g/11 ms, Half-sine shock pulse Storage/transport: 50g, Half-sine shock pulse
Vibration resistance according to IEC 60068-2-6	Operation/storage: 5g, 57 - 150 Hz
Free fall according to IEC 60068-2-32	1 m

Conformance with EMC Directives

Developed according to IEC 61000-6-2	
Noise emission according to EN 55022:1998 + A1:2000 + A2:2003 (interference voltage)	Class B (residential)
Noise emission according to EN 55011:1998 + A1:1999 + A2:2002 (electromagnetic interference)	Class A (industrial area)
Immunity to interference according to EN 61000-4-2 (IEC 1000-4-2) (ESD) Contact discharge: Air discharge: Indirect discharge:	Requirements acc. to DIN EN 61000-6-2 Test intensity 2, criterion B Test intensity 3, criterion B Test intensity 2, criterion B
Noise immunity according to EN 61000-4-3 (IEC 1000-4-3) (electromagnetic fields)	Requirements according to DIN EN 61000-6-2 Test intensity 3, criterion A
Noise immunity according to EN 61000-4-4 (IEC 1000-4-4) (burst) Data cables: Power supply:	Requirements according to DIN EN 61000-6-2 Test intensity 2, criterion B Test intensity 3, criterion B

Conformance with EMC Directives (Fortsetzung)	
Immunity to interference according to EN 61000-4-5 (IEC 1000-4-5) (surge)	Requirements according to DIN EN 61000-6-2
Data cables:	Test intensity 2, criterion B
Power supply:	Test intensity 1, criterion B
Noise immunity according to EN 61000-4-6 (IEC 1000-4-6) (conducted)	Requirements according to DIN EN 61000-6-2 Test intensity 3, criterion A

Additional certifications	
RoHS	EEE 2002/95/EC. - WEEE 2002/96/EC

9.3 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 RJ 45 I full duplex I auto MDIX
Other interfaces	Serial via USB connection
Drives	–
High availability	Depending on the firmware used
Power supply	Via USB interface (5 V at 500 mA) Option: external power supply unit (110 V ... 230 V)
Power consumption	2.5 W, maximum
Temperature range	0°C ... +40°C (operation) -20°C ... +70°C (storage)
Humidity range	20% ... 90% during operation, no condensation
Degree of protection	IP30
Dimensions (H x W x D)	27 x 77 x 115 mm
Weight	158 g

Firmware and power values	
Firmware compatibility	FL MGUARD v7.2 or later; Innominate recommends firmware Version 7.x to be used with the up-to-date patch releases; For the scope of functions, please refer tot he relevant firmware data sheet.
Data throughput (router I firewall)	up to 60 Mbps (bidirectional) I up to 40 Mbps (bidirectional)
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	up to 25 Mbps bidirectional
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	
Conformance	CE | FCC
Special features	Realtime clock | Trusted Platform Module (TPM) | temperature sensor

9.4 FL MGUARD SMART

FL MGUARD SMART /266 | FL MGUARD SMART /533

Hardware properties	
Platform	Intel network processor either with 533 MHz or 266 MHz clocking
Network interfaces	1 LAN port | 1 WAN port Ethernet IEEE 802.3 10/100 Base TX | RJ 45 | full duplex | auto MDIX
Other interfaces	–
Drives	–
High availability	Depending on the firmware used
Power supply	Via USB interface (5 V at 500 mA) Option: external power supply unit (110 V ... 230 V)
Power consumption	2.5 W, maximum
Temperature range	0°C ... +40°C (operation) -20°C ... +70°C (storage)
Humidity range	20% ... 90% during operation, no condensation
Degree of protection	IP30
Dimensions (H x W x D)	27 x 77 x 115 mm
Weight	158 g

Firmware and power values	
Firmware compatibility	FL MGUARD v5.0 or later; Innominate recommends firmware Version 6.x or 7.x to be used with the up-to-date patch releases; For the scope of functions, please refer tot he relevant firmware data sheet.
Data throughput (router | firewall) 533 MHz	up to 90 Mbps bidirectional | up to 70 Mbps bidirectional
Hardware-based encryption	DES | 3DES | AES-128/192/256
Encrypted VPN throughput (AES-256)	up to 35 Mbps (FL MGUARD SMART /256) bidirectional | up to 70 Mbps (FL MGUARD SMART /533) bidirectional
Management support	Web GUI (HTTPS) | command line interface (SSH) | SNMP v1/2/3 | central device management software
Diagnostics	LEDs: (3 LEDs in combination for boot process, heartbeat, system error, Ethernet status, recovery mode) | log file | remote syslog

Other	
Conformance	CE | FCC

9.5 FL MGUARD PCI

FL MGUARD PCI /266 | FL MGUARD PCI /533

Hardware properties	
Platform	Intel network processor either with 266 MHz or 533 MHz clocking
Network interfaces	1 LAN port	1 WAN port Ethernet IEEE 802.3 10/100 Base TX | RJ 45	full duplex	auto MDIX
Other interfaces	Serial RS-232, internal connector
Drives	–
High availability	Depending on the firmware used
Power supply	3.3 V or 5 V, via PCI bus
Power consumption	3.7 W ... 4.2 W, typical
Humidity range	20% ... 90% during operation, no condensation
Degree of protection	Depending on installation type
Temperature range	0°C ... +70°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	Low profile PCI
Weight	72 g

Firmware and power values	
Firmware compatibility	FL MGUARD v5.0 or later; Innominate recommends firmware Version 6.x or 7.x to be used with the up-to-date patch releases; For the scope of functions, please refer tot he relevant firmware data sheet.
Data throughput (router	firewall) 533 MHz	up to 99 Mbps bidirectional	up to 70 Mbps bidirectional
Hardware-based encryption	DES	3DES	AES-128/192/256
Encrypted VPN throughput (AES-256)	up to 35 Mbps (PCI /256) bidirectional | up to 70 Mbps (PCI /533) bidirectional
Management support	Web GUI (HTTPS)	command line interface (SSH)	SNMP v1/2/3	central device management software
Diagnostics	LEDs (2 x LAN, 2 x WAN in combination for boot process, heartbeat, system error, Ethernet status, recovery mode)	log file	remote syslog

Other	
Conformance	CE	FCC	UL 508 | Operating modes with/without driver via PoPCI

9.6 FL MGUARD BLADE

FL MGUARD BLADE /533

Hardware properties	
Platform	Intel network processor with 533 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I full duplex I auto MDIX
Other interfaces	Serial RS-232, RJ11 female connector
Drives	–
High availability	Depending on the firmware used
Power supply	Via *BLADEBASE*: 100 V AC ... 240 V AC at 50/60 Hz
Power consumption	*BLADE:* 3 W, typical *BLADEBASE:* 42 W, typical
Humidity range	10% ... 95% during operation, no condensation
Degree of protection	IP20
Temperature range	+5°C ... +40°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	*BLADE*: 100 x 26 x 160 mm *BLADEBASE*: 133 x 483 x 235 mm (3 HU)
Weight	*BLADE*: 245 g I *BLADEPACK*: 7.7 kg

Firmware and power values	
Firmware compatibility	FL MGUARD v5.0 or later; Innominate recommends firmware Version 6.x or 7.x to be used with the up-to-date patch releases; For the scope of functions, please refer tot he relevant firmware data sheet.
Data throughput (router I firewall)	up to 90 Mbps bidirectional I up to 70 Mbps bidirectional
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	up to 70 Mbps (BLADE /533) bidirectional
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (2 x LAN, 2 x WAN in combination for boot process, heartbeat, system error, Ethernet status, recovery mode) I log file I remote syslog

Other	
Conformance	CE I FCC

9.7 FL MGUARD DELTA

Hardware properties	
Platform	Intel network processor with 533 MHz clocking
Network interfaces	4 LAN ports, unmanaged switch I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ 45 I full duplex I auto MDIX
Other interfaces	Serial RS-232, 9-pos. D-SUB male connector
Drives	–
High availability	Depending on the firmware used
Power supply	External power supply unit 5 V/3 A, DC I 110 V ... 230 V, AC
Power consumption	4.5 W, typical
Humidity range	5% ... 95% during operation, no condensation
Degree of protection	IP20
Temperature range	0°C ... +40°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	30 x 239 x 156 mm
Weight	1300 g

Firmware and power values	
Firmware compatibility	FL MGUARD v5.0 or later; Innominate recommends firmware Version 6.x or 7.x to be used with the up-to-date patch releases; For the scope of functions, please refer tot he relevant firmware data sheet.
Data throughput (router I firewall)	up to 90 Mbps bidirectional I up to 70 Mbps bidirectional
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	up to 70 Mbps (bidirectional)
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	7 LEDs (Power, Status, WAN, LAN 1 – 4) I log file I remote syslog

Other	
Conformance	CE I FCC

9.8 Ordering data

9.8.1 Products

Description	Order designation	Order No.	Pcs./Pkt.
Industrial router	FL MGUARD RS-B	2989899	1
Industrial firewall/router	FL MGUARD RS	2989310	1
Industrial firewall/router with VPN support	FL MGUARD RS VPN	2989611	1
Industrial firewall/router with VPN support and integrated analog modem	FL MGUARD RS VPN ANALOG	2989718	1
Industrial firewall/router with VPN support and integrated ISDN terminal adapter	FL MGUARD RS VPN ISDN	2989815	1
Industrial firewall/router in PCI card format, 266 MHz	FL MGUARD PCI/266	2989019	1
Industrial firewall/router in PCI card format, 266 MHz and VPN support	FL MGUARD PCI/266 VPN	2989514	1
Industrial firewall/router in PCI card format, 533 MHz	FL MGUARD PCI/533	2989213	1
Industrial firewall/router in PCI card format, 533 MHz and VPN support	FL MGUARD PCI/533 VPN	2989417	1
Industrial firewall/router with Gigabit	FL MGUARD GT/GT	2700197	1
Industrial firewall/router with Gigabit and VPN	FL MGUARD GT/GT VPN	2700198	1
Replaceable configuration memory	FL MEM PLUG	2891259	1
SFP slot module in SFP format - multi-mode	FL SFP SX	2891754	1
SFP slot module in SFP format - single-mode	FL SFP LX	2891767	1
SFP slot module in SFP format - single-mode long haul	FL SFP LX LH	2989912	1

9.8.2 Accessories

Description	Order designation	Order No.	Pcs./Pkt.
Universal end clamp	E/NS 35 N	0800886	1
Network monitoring with HMI/SCADA systems	FL SMNP OPC SERVER	2832166	1
Patchbox 8 x RJ45 CAT5e, pre-assembled, can be retrofitted	FL PBX 8TX	2832496	1
Patchbox 6 x RJ45 CAT5e and 4 SC-RJ, glass, pre-assembled, can be retrofitted	FL PBX 6TX/4FX	2832506	1
Angled patch connector with two RJ45 CAT5e network connections including Layer 1 security elements	FL PF SEC 2TX	2832687	1
Angled patch connector with eight RJ45 CAT5e network connections including Layer 1 security elements	FL PF SEC 8TX	2832690	1
Angled patch connector with two RJ45 CAT5e network connections	FL PF 2TX CAT5E	2891165	1
Angled patch connector with eight RJ45 CAT5e network connections	FL PF 8TX CAT5E	2891178	1
Angled patch connector with two RJ45 CAT6 network connections	FL PF 2TX CAT 6	2891068	1
Angled patch connector with eight RJ45 CAT6 network connections	FL PF 8TX CAT 6	2891071	1
Patch cable, CAT**6**, pre-assembled, 0.3 m long	FL CAT6 PATCH 0,3	2891181	10
Patch cable, CAT**6**, pre-assembled, 0.5 m long	FL CAT6 PATCH 0,5	2891288	10
Patch cable, CAT**6**, pre-assembled, 1.0 m long	FL CAT6 PATCH 1,0	2891385	10
Patch cable, CAT**6**, pre-assembled, 1.5 m long	FL CAT6 PATCH 1,5	2891482	10
Patch cable, CAT**6**, pre-assembled, 2.0 m long	FL CAT6 PATCH 2,0	2891589	10
Patch cable, CAT**6**, pre-assembled, 3.0 m long	FL CAT6 PATCH 3,0	2891686	10
Patch cable, CAT**6**, pre-assembled, 5.0 m long	FL CAT6 PATCH 5,0	2891783	10

Description (Fortsetzung)	Order designation	Order No.	Pcs./Pkt.
Patch cable, CAT**6**, pre-assembled, 7.5 m long	FL CAT6 PATCH 7,5	2891880	10
Patch cable, CAT**6**, pre-assembled, 10 m long	FL CAT6 PATCH 10	2891887	10
Patch cable, CAT**6**, pre-assembled, 12.5 m long	FL CAT6 PATCH 12,5	2891369	5
Patch cable, CAT**6**, pre-assembled, 15 m long	FL CAT6 PATCH 15	2891372	5
Patch cable, CAT**6**, pre-assembled, 20 m long	FL CAT6 PATCH 20	2891576	5
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 marker for FL PATCH GUARD, black	FL PATCH GUARD CCODE BK	2891136	12
Color marker for FL PATCH GUARD, blue	FL PATCH GUARD CCODE BU	2891233	12
Color marker for FL PATCH GUARD, green	FL PATCH GUARD CCODE GN	2891631	12
Color marker for FL PATCH GUARD, orange	FL PATCH GUARD CCODE OG	2891330	12
Color marker for FL PATCH GUARD, red	FL PATCH GUARD CCODE RD	2891738	12
Color marker 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 marker 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 CAT 5/6 PATCH ...	FL PATCH SAFE CLIP	2891246	20

HOTLINE:

If there are any problems that cannot be solved with the help of this documentation, please contact our hotline: +49 - 52 81 - 94 62 88 8