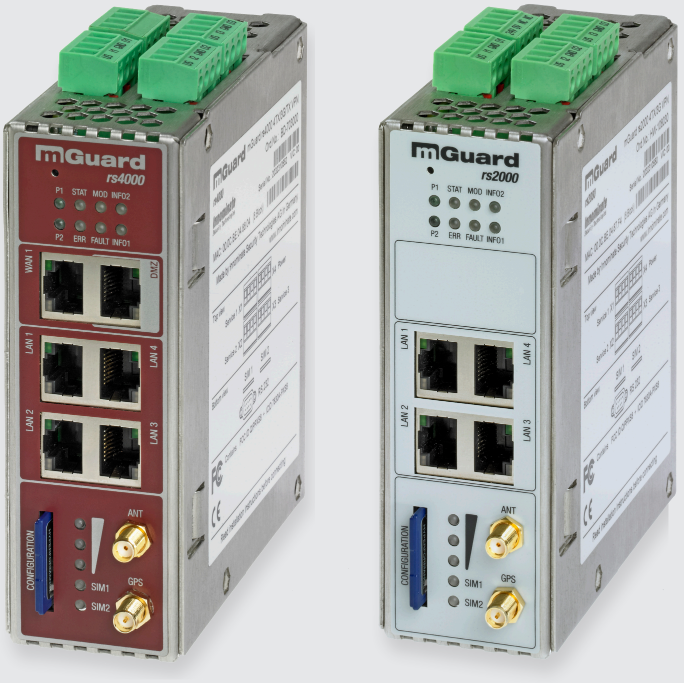
mGuard

Configuration of the mGuard Security Appliances

Hardware Reference Manual



Innominate
Security Technologies

User manual

Installing and starting up the mGuard hardware

2015-07-24

Designation: UM EN MGUARD DEVICES

Revision: 02

Order No.: —

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

- mGuard rs4000/rs2000
  - rs4000 TX/TX
  - rs4000 TX/TX VPN
  - rs2000 TX/TX VPN
- mGuard rs4000/rs2000 Switch
  - rs4000 4TX/TX
  - rs4000 4TX/TX VPN
  - rs2000 5TX/TX VPN
- mGuard rs4000/rs2000 3G
  - rs4000 4TX/3G/TX VPN
  - rs2000 4TX/3G VPN
- mGuard smart^2/smart
- mGuard pci^2 SD
- mGuard pcie^2 SD
- mGuard pci
- mGuard blade
- mGuard delta^2
- mGuard delta
- mGuard centerport^2
- mGuard centerport
- mGuard industrial rs
- EAGLE mGuard

Please observe the following notes

Target group of this user manual

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

Explanation of symbols used and signal words

⚠ This symbol indicates hazards that could lead to personal injury. Obey all safety measures that follow this symbol to avoid possible injury or death.

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

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

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

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

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

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

General terms and conditions of use for technical documentation

Innominate 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 changes that serve the purpose of technical progress.

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

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

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

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

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

Published by

Innominate Security Technologies AG

Rudower Chaussee 13
12489 Berlin
Germany
Phone: +49 (0)30 92 10 28-0
contact@innominate.com

www.innominate.com

Notes on CE identification

The declarations of conformity are held here in agreement with EU directives for the relevant authorities:

Innominate Security Technologies AG
Rudower Chaussee 13
12489 Berlin
Germany
Tel. +49 (0)30 92 10 28-0

FCC Note

The FCC Statement applies to the following devices:

Class A: mGuard rs4000, mGuard rs2000, mGuard rs4000 Switch, mGuard rs2000 Switch, mGuard centerport, mGuard industrial rs, mGuard smart^2, mGuard smart, mGuard pci, mGuard pci^2 SD, mGuard delta, mGuard delta^2, and EAGLE mGuard. **Class B:** mGuard rs4000 3G, mGuard rs2000 3G, mGuard centerport^2

FCC Statement

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

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

Table of contents

1 mGuard rs4000/rs2000

Table 1-1 Available mGuard rs4000/rs2000 versions

Available versions	Order No.
mGuard rs4000 TX/TX	HW-107010
mGuard rs4000 TX/TX VPN	BD-701000
mGuard rs2000 TX/TX VPN	HW-108010

The **mGuard rs4000** is a security router with intelligent firewall and optional IPsec VPN (10 to 250 tunnels). It has been designed for use in industry to accommodate strict distributed security and high availability requirements.

The **mGuard rs2000** is a version with basic firewall and integrated IPsec VPN (maximum of two tunnels). Its scope of functions is reduced to the essentials. It is suitable for secure remote maintenance applications in industry and enables the quick startup of robust field devices for industrial use, thereby facilitating error-free, independent operation.

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

The following connectivity options are available

mGuard rs4000: (LAN/WAN)		**mGuard rs2000: (LAN/WAN)**	
TX/TX	Ethernet/Ethernet	TX/TX VPN	Ethernet/Ethernet + VPN
TX/TX VPN	Ethernet/Ethernet + VPN		

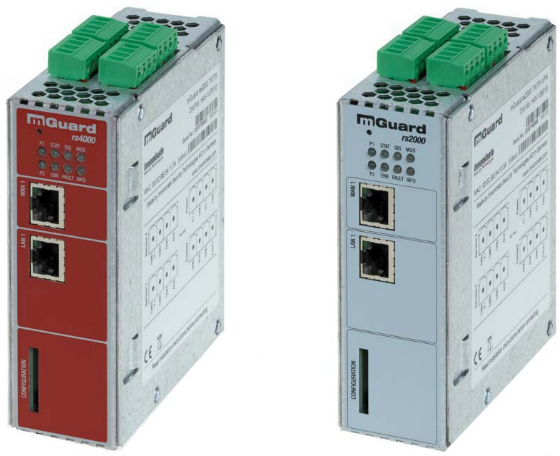


Figure 1-1 mGuard rs4000/mGuard rs2000

1.1 Operating elements and LEDs

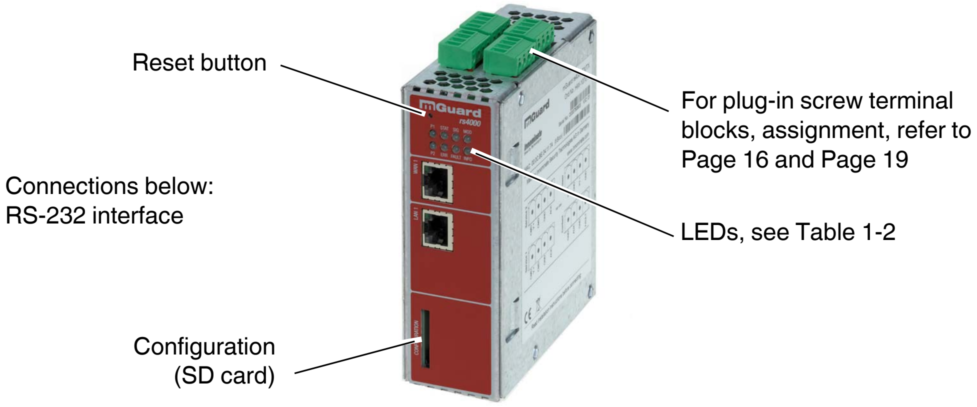


Figure 1-2 Operating elements and LEDs on the mGuard rs4000

Table 1-2 LEDs on the mGuard rs4000 and mGuard rs2000

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active (mGuard rs2000: not used)
STAT	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
ERR	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see Page 28) or contact your dealer.
STAT+ ERR	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
SIG	–		(Not used)
FAULT	Red	On	The signal output takes low level due to an error (inverted logic) (see Page 17 or Page 18). The signal output is inactive during a restart.
MOD	Green	On	Connection via modem established

Table 1-2 LEDs on the mGuard rs4000 and mGuard rs2000 [...]

LED	State		Meaning
INFO	Green	On	Up to firmware version 8.0: the configured VPN connection has been established As of firmware version 8.1, the configured VPN connections are established or the firewall rule records defined at output O1 are activated
		Flashing	Up to firmware version 8.0: the configured VPN connection is being established or aborted As of firmware version 8.1: the configured VPN connections are being established or aborted or the defined firewall rule records are activated or deactivated.
LAN	Green	On	The LAN/WAN LEDs are located in the LAN/WAN sockets (10/100 and duplex LED) **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	

1.2 Startup

1.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

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

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

NOTE: Cleaning

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

1.2.2 Checking the scope of supply

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

The scope of supply includes:

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

1.3 Installation of mGuard rs4000/rs2000

1.3.1 Mounting/removal

Mounting

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

- Mount the mGuard rs4000/rs2000 on a grounded 35 mm DIN rail according to DIN EN 60715.

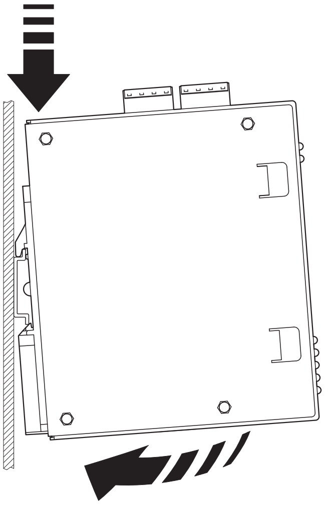


Figure 1-3 Mounting the mGuard rs4000/rs2000 on a DIN rail

- Attach the top snap-on foot of the mGuard rs4000/rs2000 to the DIN rail and then press the mGuard rs4000/rs2000 down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the mGuard rs4000/rs2000 from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the mGuard rs4000/rs2000.

1.3.2 Connecting to the network

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

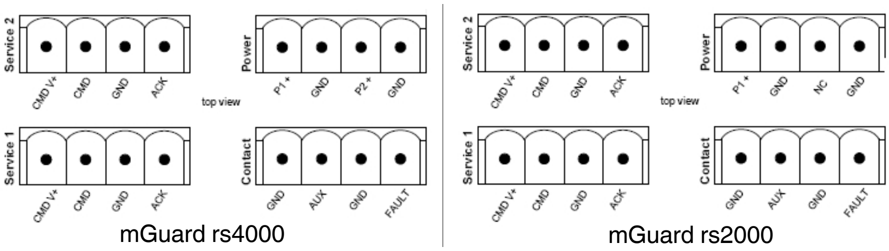
- Connect the mGuard to the network. To do this, you need a suitable UTP cable (CAT5) which is not included in the scope of supply.
- Connect the internal network interface LAN 1 of the mGuard to the corresponding Ethernet network card of the configuration computer or a valid network connection of the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

1.3.3 Service contacts

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

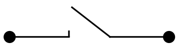
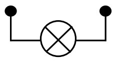
Please note that only the “Service 1” contacts are used with firmware version up to and including 7.6x. The “Service 2” contacts shall be made available as of firmware version 8.1.

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



mGuard rs4000

mGuard rs2000

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

	P1+	GND	P2+	GND
Power	+24 V	0 V	+24 V	0 V
	See Section 1.3.4		Only for mGuard rs4000 See Section 1.3.4	

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

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

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

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

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

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

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

Service contacts as of firmware version 8.1

Input/CMD I1, CMD I2

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

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

Operating a connected push button

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

Operating a connected on/off switch

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

Signal contact (signal output) ACK O1, O2

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

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

Alarm output ACK O3

The O3 alarm output monitors the function of the mGuard rs4000/rs2000 and therefore enables remote diagnostics.

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

The O3 alarm output reports the following when “Management, Service I/O, Alarm output” has been activated.

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

Service contacts up to firmware version 8.0

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

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

Operating a connected push button

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

Operating a connected on/off switch

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

INFO LED

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

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

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

Signal contact (signal output)

The signal contact monitors the function of the mGuard rs4000/rs2000 and thus enables remote diagnostics.

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

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

- Failure of at least one of the two supply voltages.
- Power supply of the mGuard rs4000/rs2000 below the limit value (supply voltage 1 and/or 2 lower than 11 V).
- Link status monitoring of the Ethernet connections, if configured. By default upon delivery, the connection is not monitored. Monitoring can be activated (on the web interface under “Management >> System Settings >> Signal Contact”).
- Error during selftest.

During a restart, the signal contact is switched off until the mGuard rs4000/rs2000 has started up completely. This also applies when the signal contact is manually set to “Closed” under “Manual settings” in the software configuration.

1.3.4 Connecting the supply voltage

WARNING: The mGuard rs4000/rs2000 is designed for operation with a DC voltage of 11 V DC ... 36 V DC/SELV, 1.5 A, maximum.

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

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

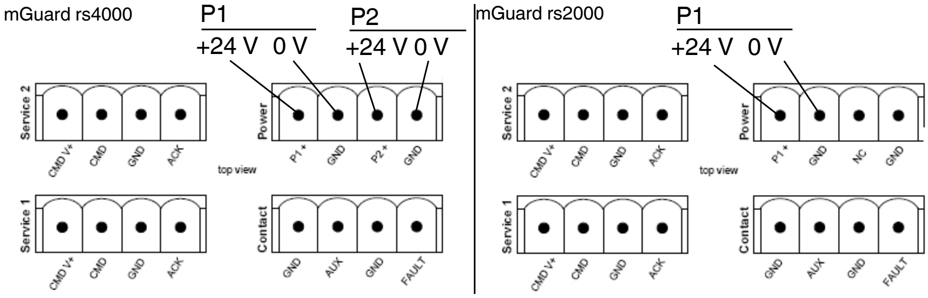


Figure 1-4 Connecting the supply voltage

The mGuard rs4000 has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Do not connect the service contacts to an external voltage source.
- Wire the supply voltage lines with the corresponding screw terminal block (P1/P2) of the mGuard. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the screw terminal blocks into the intended sockets on the top of the mGuard (see Figure 1-4).

Status LED P1 lights up green when the supply voltage has been connected properly. On the mGuard rs4000, the status indicator P2 also lights up if there is a redundant supply voltage connection.

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

Redundant voltage supply (mGuard rs4000)

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the mGuard rs4000 alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the mGuard rs4000 indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs (P1/P2) or by installing an appropriate wire jumper between connections P1 and P2.

1.4 Preparing the configuration

1.4.1 Connection requirements

- The **mGuard rs4000/rs2000** must be connected to at least one active power supply unit.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the mGuard.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

1.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 1-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard rs4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard rs2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 24). Alternatively, you can select a different stealth configuration or use another network mode.

1.5 Configuration in Stealth mode

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

- https://192.168.1.1/ (see Page 22)
- https://1.1.1.1/ (see Page 22)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 23).

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

Computers can access the mGuard via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the mGuard. For this purpose, the 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 product can no longer be accessed via IP address 192.168.1.1.

1.5.1 IP address 192.168.1.1

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

– The mGuard is in the delivery state.

– The mGuard was reset to the default settings via the web interface and restarted.

– The rescue procedure (flashing of the mGuard) or the recovery procedure has been performed.

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

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

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

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

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

1.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the 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 and if the default gateway can be accessed via the WAN port of the mGuard at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 24). Continue from this point.

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

1.5.3 Assigning the IP address via BootP

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

For IP address assignment, the 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.

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

Notes for BootP

During initial startup, the mGuard transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the mGuard no longer sends BootP requests. The product can then no longer be accessed via IP address 192.168.1.1.

After receiving a BootP reply, the mGuard no longer sends BootP requests, not even after it has been restarted. For the 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 mGuard is connected to a computer using a Microsoft Windows operating system.

1.6 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 1-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard rs4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard rs2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 1-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 28).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 20).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

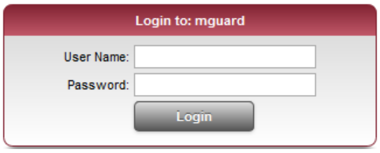


Figure 1-5 Login

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

User Name:	admin
Password:	mGuard

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

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

1.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

Configuration

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

1.8 Restart, recovery procedure, and flashing the firmware

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

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

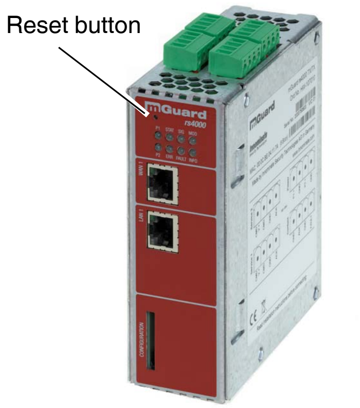


Figure 1-6 Reset button

1.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

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

1.8.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 1-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard rs4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
mGuard rs2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

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

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.

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

– The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The mGuard is in Router or PPPoE mode.

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

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

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

1.8.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

> **NOTE:** During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.
>
> The following requirements apply when loading the firmware from an SD card:
>
> - All necessary firmware files must be located in a common directory on the first partition of the SD card
> - This partition must use a VFAT file system (standard type for SD cards).
>
> To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 258).

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

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

  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s

Action

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

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

- Hold down the Reset button until the STAT, MOD, and SIG LEDs light up green. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The STAT LED flashes.

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

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

  The STAT, MOD, and SIG LEDs form a running light.

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

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

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

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

- Restart the mGuard. To do this, briefly press the Reset button.

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

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 24).

1.9 Technical data

Hardware properties	mGuard rs4000	mGuard rs2000
Platform	Freescale network processor with 330 MHz clocking	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 I full duplex I auto MDIX	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232 I D-SUB 9 connector 2 digital inputs and 2 digital outputs	Serial RS-232 I D-SUB 9 connector 2 digital inputs and 2 digital outputs
Memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory	128 MB RAM I 128 MB Flash I SD card Replaceable configuration memory
Redundancy options	Optional: VPN I router and firewall	Not available
Power supply	Voltage range 11 ... 36 V DC, redundant	Voltage range 11 ... 36 V DC
Power consumption	2.13 W, typical	2.13 W, typical
Humidity range	5% ... 95% (operation, storage), non-condensing	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20	IP20
Temperature range	-20°C ... +60°C (operation) -20°C ... +60°C (storage)	-20°C ... +60°C (operation) -20°C ... +60°C (storage)
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)	130 x 45 x 114 mm (up to DIN rail support)
Weight	725 g (TX/TX)	722 g (TX/TX)

Firmware and power values	mGuard rs4000	mGuard rs2000
Firmware compatibility	For mGuard v7.4.0 or later: Innominate recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.	
Data throughput (router I firewall)	Router mode, default firewall rules, bidirectional throughput: 99 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum.	
Virtual Private Network (VPN)	IPsec (IETF standard) Up to 250 VPN tunnels	IPsec (IETF standard) Up to 2 VPN tunnels
Hardware-based encryption	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: 35 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 25 Mbps, maximum	
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software	
Diagnostics	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) signal contacts I service contacts I log file I remote syslog	LEDs (Power, State, Error, Signal, Fault, Modem, Info) signal contacts I service contacts I log file I remote syslog

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

2 mGuard rs4000/rs2000 Switch

Table 2-1 Available mGuard rs4000/rs2000 Switch versions

Available versions	Order No.
mGuard rs4000 4TX/TX	HW-107020
mGuard rs4000 4TX/TX VPN	BD-702000
mGuard rs2000 5TX/TX VPN	HW-108020

The **mGuard rs4000 Switch** is suitable for distributed protection of production cells or individual machines against manipulation.

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

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

For software-independent remote maintenance, the mGuard rs4000 Switch can be used as a VPN router for up to 250 parallel, IPsec-encrypted VPN tunnels.

The **mGuard rs2000 Switch** is a version with basic firewall and can be used as a VPN client for up to two parallel, IPsec-encrypted VPN tunnels. It is suitable for secure remote maintenance applications and enables connection of globally distributed machines and controllers.

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

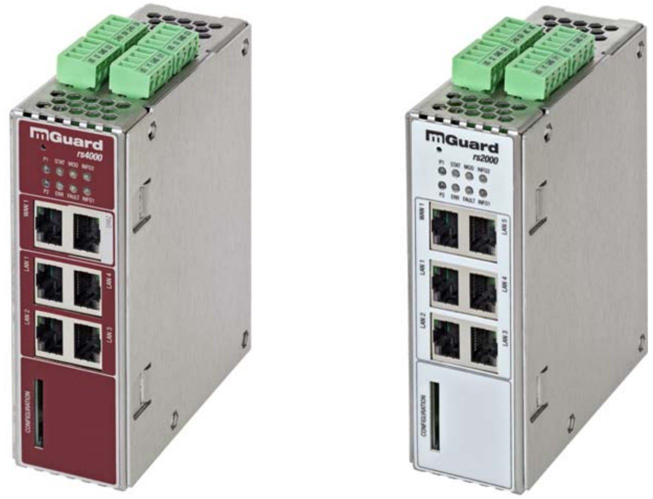


Figure 2-1 mGuard rs4000 Switch/mGuard rs2000 Switch

2.1 Operating elements and LEDs

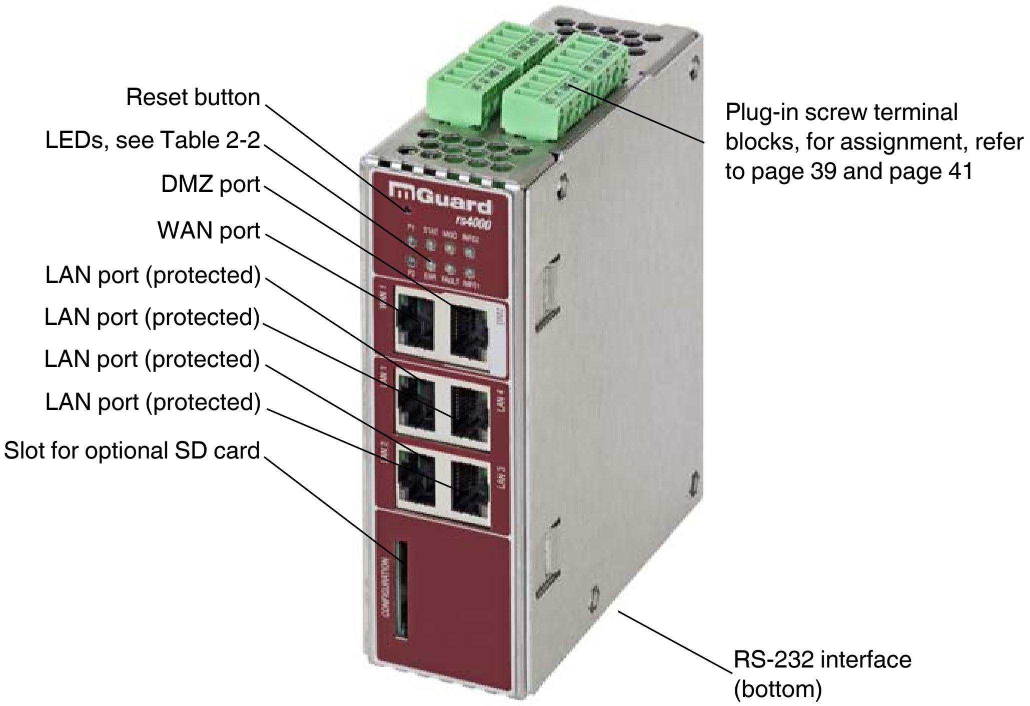


Figure 2-2 Operating elements and LEDs on the mGuard rs4000 Switch

Table 2-2 LEDs on the mGuard rs4000 Switch and mGuard rs2000 Switch

LED	State		Meaning			
P1	Green	On	Power supply 1 is active			
P2	Green	On	Power supply 2 is active (mGuard rs2000 Switch: not used)			
Stat	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.			
Err	Red	Flashing	**System error**. Restart the device. – Press the reset button shortly (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see page 47) or contact your dealer.			
Stat + Err	Flashing alternately: green and red		**Boot process**. When the device has been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.			
Mod	Green	On	Connection via modem established			
Fault	Red	On	The signal output takes low level due to an error (inverted logic). The signal output is inactive during a restart.			

Table 2-2 LEDs on the mGuard rs4000 Switch and mGuard rs2000 Switch [...]

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

[1] mGuard rs4000 Switch only

[2] mGuard rs2000 Switch only

2.2 Startup

2.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

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

NOTE: Risk of damage to equipment due to noise emissions

This is a Class A item of equipment. This equipment can cause radio interference in residential areas; in this case, the operator may be required to implement appropriate measures.

NOTE: Electrostatic discharge

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

General notes regarding usage

NOTE: Select suitable ambient conditions

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

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

NOTE: Cleaning

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

2.2.2 Checking the scope of supply

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

The scope of supply includes:

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

2.2.3 mGuard-Firmware

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

2.3 Installing the mGuard rs4000/rs2000 Switch

2.3.1 Mounting/removal

NOTE: Device damage

Only mount and remove devices when the power supply is disconnected.

Mounting

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

- Mount the mGuard rs4000/rs2000 Switch on a grounded 35 mm DIN rail according to DIN EN 60715.

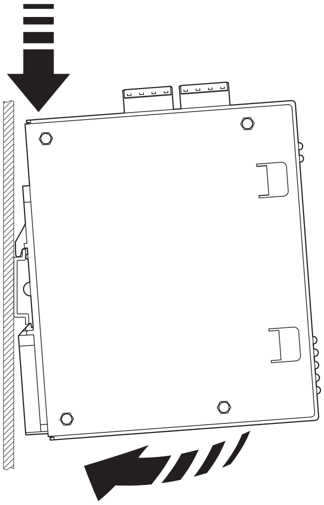


Figure 2-3 Mounting the mGuard rs4000/rs2000 Switch on a DIN rail

- Attach the top snap-on foot of the mGuard rs4000/rs2000 Switch to the DIN rail and then press the mGuard rs4000/rs2000 Switch down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the mGuard rs4000/rs2000 Switch from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the mGuard rs4000/rs2000 Switch.

2.3.2 Connecting to the network

NOTE: Risk of material damage due to incorrect wiring

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

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

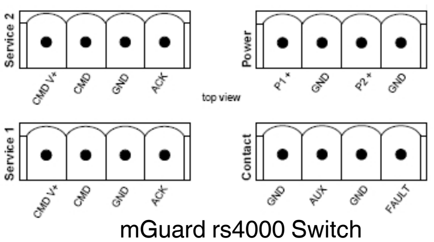
2.3.3 Connecting the service contacts

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

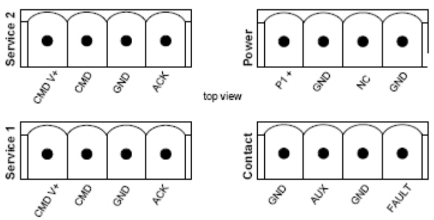
The plug-in screw terminal blocks of the service contacts may be removed or inserted during operation of the device.

The mGuard rs4000/rs2000 Switch has three digital inputs and outputs. These are configured in the web interface, e.g., as a control signal for starting and stopping VPN connections.

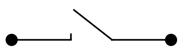
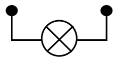
The digital inputs and outputs are connected as follows.



mGuard rs4000 Switch



mGuard rs2000 Switch

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

	P1+	GND	P2+	GND
Power	+24 V	0 V	+24 V	0 V
	See Section 2.3.4		Only for mGuard rs4000 See Section 2.3.4	

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

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

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

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

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

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

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

Service contacts as of firmware version 8.1

Input/CMD I1, CMD I2

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

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

Operating a connected push button

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

Operating a connected on/off switch

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

Signal contact (signal output) ACK O1, O2

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

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

Alarm output ACK O3

The O3 alarm output monitors the function of the mGuard rs4000/rs2000 and therefore enables remote diagnostics.

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

The O3 alarm output reports the following when “Management, Service I/O, Alarm output” has been activated.

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

2.3.4 Connecting the supply voltage

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

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

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

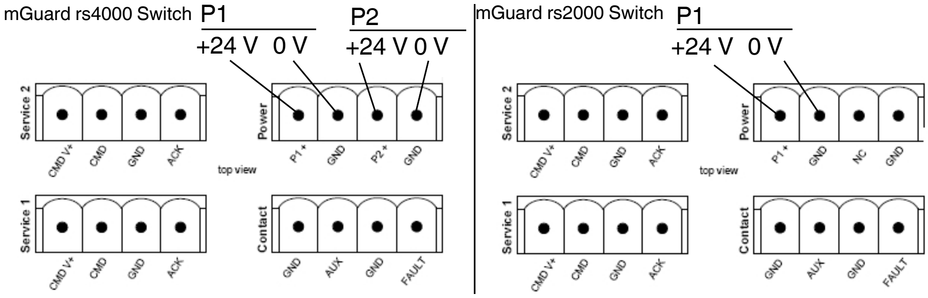


Figure 2-4 Connecting the supply voltage

The mGuard rs4000 Switch has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

- Remove the plug-in screw terminal blocks for the power supply and the service contacts.
- Wire the supply voltage lines with the corresponding screw terminal block (P1/P2) of the mGuard. Tighten the screws on the screw terminal blocks with 0.5 ... 0.8 Nm.
- Insert the plug-in screw terminal blocks into the intended sockets on the top of the device.

The P1 status LED lights up green when the supply voltage has been connected properly. On the mGuard rs4000 Switch, the P2 LED also lights up if there is a redundant supply voltage connection.

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

Redundant power supply (mGuard rs4000 Switch)

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 mGuard rs4000 Switch alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the mGuard rs4000 Switch indicates the failure of one supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs or by installing an appropriate wire bridge between the connections.

2.4 Preparing the configuration

2.4.1 Connection requirements

- The **mGuard rs4000/rs2000 Switch** must be connected to at least one active power supply unit.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the device.
- **For remote configuration**: The device must be configured so that remote configuration is permitted.
- The device must be connected, i.e., the required connections must be working.

2.5 Configuration in Router mode

On initial startup, the mGuard can be accessed via the following address:

- https://192.168.1.1

2.5.1 IP address 192.168.1.1

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

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

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

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

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

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

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

–

2.6 Establishing a local configuration connection

Web-based administrator interface

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

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

The device can be accessed via the following address:

Table 2-3 Preset address

Default setting	Network mode	Management IP #1
mGuard rs2000 Switch	Router	https://192.168.1.1/
mGuard rs4000 Switch	Router	https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the device completely into the address line of the web browser (refer to Table 2-3).

You access the administrator website of the device.

If the administrator web page of the device cannot be accessed

If you have forgotten the configured address

If the address of the device in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the device must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 47).

If the administrator web page is not displayed

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

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

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

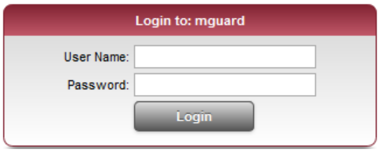


Figure 2-5 Login

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

User Name:	admin
Password:	mGuard

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

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

2.7 Remote configuration

Requirement

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

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

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the device can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the device can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer: https://123.45.67.89/

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

Configuration

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

2.8 Restart, recovery procedure, and flashing the firmware

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

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

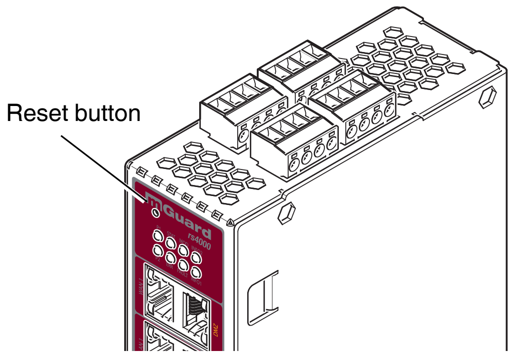


Figure 2-6 Reset button

2.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

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

2.8.2 Performing a recovery procedure

Objective

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

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

The following network setting is restored:

Table 2-4 Restored network setting

Network mode	Management IP #1	Management IP #2
Router		https://192.168.1.1/

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

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

Possible reasons for performing the recovery procedure:

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

> Up-to-date information on the recovery and flashing procedure can be found in the application note for your firmware version.
>
> You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

2.8.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

> **NOTE:** During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.
>
> The following requirements apply when loading the firmware from an SD card:
>
> - All necessary firmware files must be located in a common directory on the first partition of the SD card
> - This partition must use a VFAT file system (standard type for SD cards)
>
> To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 258).

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

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

  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s

Action

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

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

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

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

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

  The Stat LED flashes.

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

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

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

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

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

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

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

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

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

The device is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 43).

2.9 Technical data

Hardware properties	mGuard rs4000 Switch	mGuard rs2000 Switch
Platform	Freescale network processor	Freescale network processor
Network interfaces	4 LAN ports (managed) ǀ 1 DMZ port ǀ 1 WAN port Ethernet IEEE 802.3 10/100 Base TX RJ45 ǀ full duplex ǀ auto MDIX	5 LAN ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ45 ǀ full duplex ǀ auto MDIX
Other interfaces	Serial RS-232 ǀ D-SUB 9 connector 3 digital inputs and 3 digital outputs	Serial RS-232 ǀ D-SUB 9 connector 3 digital inputs and 3 digital outputs
Memory	128-Mbyte RAM ǀ 128-Mbyte Flash SD card Replaceable configuration memory	128-Mbyte RAM ǀ 128-Mbyte Flash SD card Replaceable configuration memory
Redundancy options	Optional: VPN ǀ router and firewall	–
Power supply	Voltage range 11 ... 36 V DC, redundant	Voltage range 11 ... 36 V DC
Current consumption	Typical < 200 mA (24 V DC) ǀ Maximum < 800 mA (10 V DC)	Typical < 200 mA (24 V DC) ǀ Maximum < 800 mA (10 V DC)
Humidity range	5% ... 95% (operation, storage), non-condensing	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20	IP20
Temperature range	-20°C ... +60°C (operation) -20°C ... +70°C (storage)	-20°C ... +60°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	130 mm x 45 mm x 114 mm (up to DIN rail support)	130 mm x 45 mm x 114 mm (up to DIN rail support)
Weight	835 g	835 g

<table>
<tr><th>Firmware and power values</th><th>mGuard rs4000 Switch</th><th>mGuard rs2000 Switch</th></tr>
<tr><td>Firmware compatibility</td><td colspan="2">Firmware 8.1.5: Innominate recommends the use of the latest firmware version and patch releases in each case.
For the scope of functions, please refer to the relevant firmware data sheet.</td></tr>
<tr><td>Data throughput (router ǀ firewall)</td><td colspan="2">Router mode, default firewall rules, bidirectional throughput: 99 Mbps, maximum
Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum
When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.</td></tr>
<tr><td>Virtual Private Network (VPN)</td><td>IPsec (IETF standard)
Up to 250 VPN tunnels</td><td>IPsec (IETF standard)
Up to 2 VPN tunnels</td></tr>
<tr><td>Hardware-based encryption</td><td>DES ǀ 3DES ǀ AES-128/192/256</td><td>DES ǀ 3DES ǀ AES-128/192/256</td></tr>
<tr><td>Encrypted VPN throughput (AES-256)</td><td colspan="2">Router mode, default firewall rules, bidirectional throughput: 35 Mbps, maximum
Stealth mode, default firewall rules, bidirectional throughput: 25 Mbps, maximum
When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.</td></tr>
<tr><td>Management support</td><td colspan="2">Web GUI (HTTPS) ǀ command line interface (SSH) ǀ SNMP v1/2/3 ǀ central device management software</td></tr>
<tr><td>Diagnostics</td><td colspan="2">13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signal Status, SIM Status) ǀ service I/O ǀ log file ǀ remote Syslog</td></tr>
</table>

<table>
<tr><th>Other</th><th>mGuard rs4000 Switch</th><th>mGuard rs2000 Switch</th></tr>
<tr><td>Special features</td><td colspan="2">Realtime clock ǀ Trusted Platform Module (TPM) ǀ temperature sensor ǀ mGuard Secure Cloud ready</td></tr>
</table>

3 mGuard rs4000/rs2000 3G

Table 3-1 Available mGuard rs4000/rs2000 3G versions

Available versions	Order No.
mGuard rs4000 4TX/3G/TX VPN	BD-703000
mGuard rs2000 4TX/3G VPN	HW-108030

The **mGuard rs4000 3G** is suitable for distributed protection of production cells or individual machines against manipulation.

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

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

For software-independent remote maintenance, the mGuard rs4000 3G can be used as a VPN router for up to 250 parallel, IPsec-encrypted VPN tunnels.

The **mGuard rs2000 3G** is a version with basic firewall and can be used as a VPN client for up to two parallel, IPsec-encrypted VPN tunnels. It is suitable for secure remote maintenance applications at locations without wired networks and enables global connection of distributed machines and controllers.

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

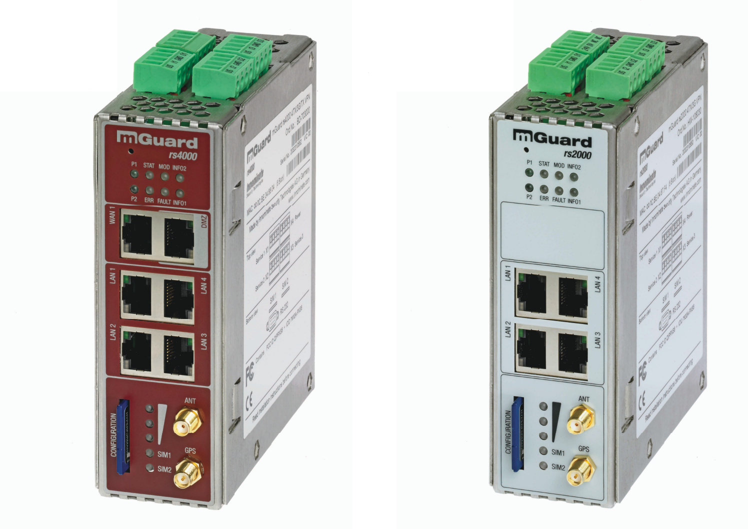


Figure 3-1 mGuard rs4000 3G/mGuard rs2000 3G

3.1 Operating elements and LEDs

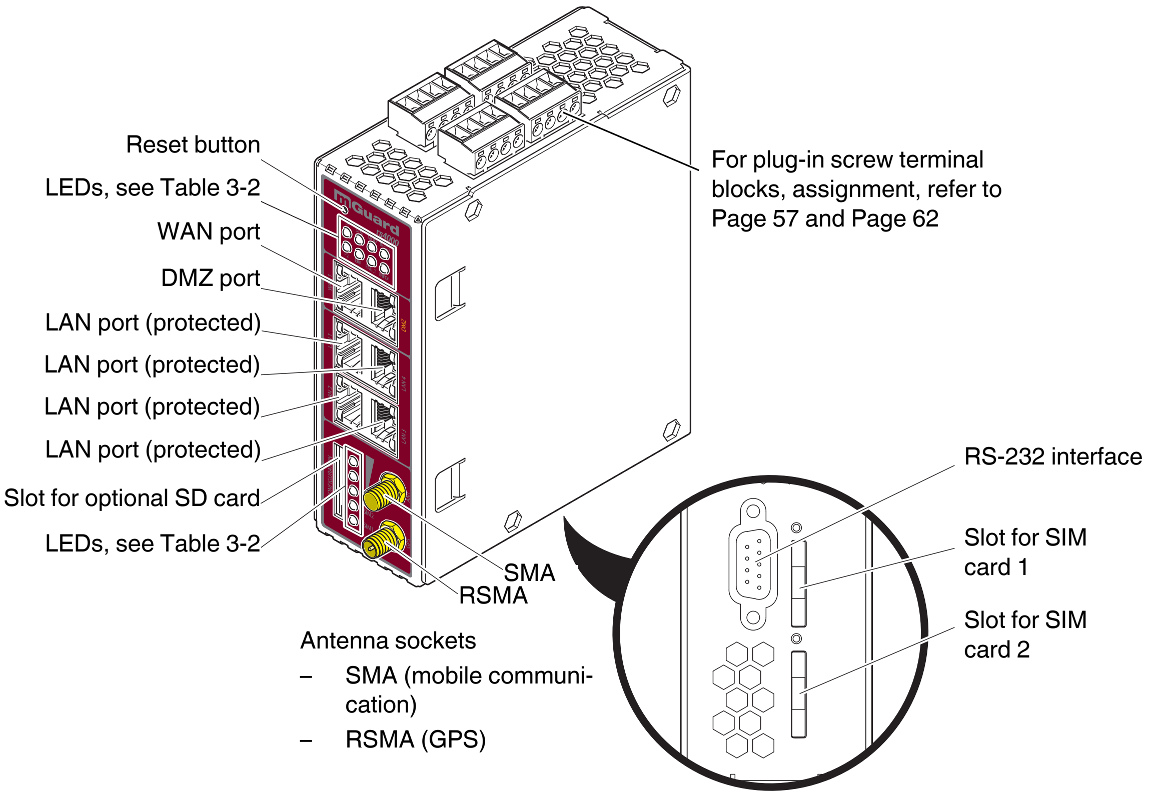


Figure 3-2 Operating elements and LEDs on the mGuard rs4000 3G

Table 3-2 LEDs on the mGuard rs4000 3G and mGuard rs2000 3G

LED	State		Meaning
P1	Green	On	Power supply 1 is active
P2	Green	On	Power supply 2 is active (mGuard rs2000 3G: not used)
Stat	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
Err	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see Page 69) or contact your dealer.
Stat + Err	Flashing alternately: green and red		**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
Mod	Green	On	Connection via modem established
Fault	Red	On	The signal output takes low level due to an error (inverted logic). The signal output is inactive during a restart.

Table 3-2 LEDs on the mGuard rs4000 3G and mGuard rs2000 3G [...]

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

* only mGuard rs4000 3G

3.2 Startup

3.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

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

NOTE: Risk of material damage due to emissions

This is a Class A item of equipment. This equipment can cause radio interference in residential areas; in this case, the operator may be required to implement appropriate measures.

NOTE: Electrostatic discharge

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

General notes regarding usage

NOTE: Select suitable ambient conditions

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

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

NOTE: Cleaning

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

3.2.2 Checking the scope of supply

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

The scope of supply includes:

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

3.2.3 mGuard-Firmware

- The device must be operated with mGuard-Firmware version 8.0 or higher.

3.3 Installation of mGuard rs4000/rs2000 3G

3.3.1 Mounting/removal

NOTE: Device damage

Only mount and remove devices when the power supply is disconnected.

Mounting

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

- Mount the mGuard rs4000/rs2000 3G on a grounded 35 mm DIN rail according to DIN EN 60715.

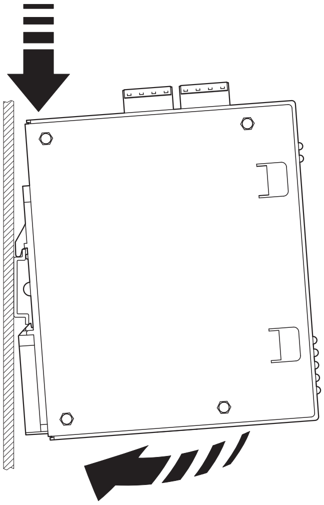


Figure 3-3 Mounting the mGuard rs4000/rs2000 3G on a DIN rail

- Attach the top snap-on foot of the mGuard rs4000/rs2000 3G to the DIN rail and then press the mGuard rs4000/rs2000 3G down towards the DIN rail until it engages with a click.

Removal

- Remove or disconnect the connections.
- To remove the mGuard rs4000/rs2000 3G from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the mGuard rs4000/rs2000 3G.

3.3.2 Connecting to the network

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

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

3.3.3 Connecting service contacts

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

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

The mGuard rs4000/rs2000 3G has three digital inputs and outputs. These are configured in the web interface, e.g., the starting and stopping of VPN, sending alarms via SMS etc..

The digital inputs and outputs are connected as follows.

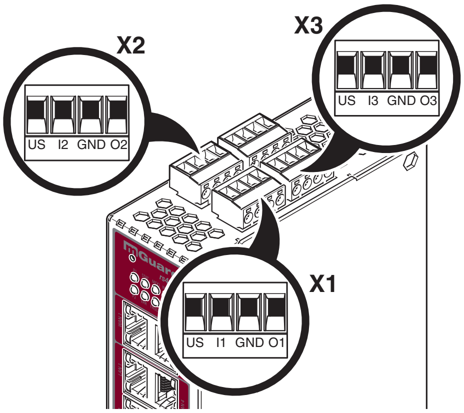
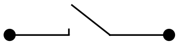
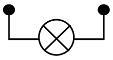


Figure 3-4 Service contacts

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

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

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

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

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

Service contacts as of firmware version 8.1

Input/CMD I1, CMD I2

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

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

Operating a connected push button

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

Operating a connected on/off switch

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

Signal contact (signal output) ACK O1, O2

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

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

Alarm output ACK O3

The O3 alarm output monitors the function of the mGuard rs4000/rs2000 and therefore enables remote diagnostics.

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

The O3 alarm output reports the following when “Management, Service I/O, Alarm output” has been activated.

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

Service contacts up to firmware version 8.0

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

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

Operating a connected push button

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

  Flashing indicates that the 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 INFO LED remains lit continuously.
- To release the VPN connection, hold down the button for a few seconds until the signal output flashes or goes out. Only then release the button.

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

Operating a connected on/off switch

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

INFO LED

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

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

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

Signal contact (signal output)

The signal contact monitors the function of the mGuard rs4000/rs2000 and thus enables remote diagnostics.

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

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

- Failure of at least one of the two supply voltages.
- Power supply of the mGuard rs4000/rs2000 below the limit value (supply voltage 1 and/or 2 lower than 11 V).
- Link status monitoring of the Ethernet connections, if configured. By default upon delivery, the connection is not monitored. Monitoring can be activated (on the web interface under “Management >> System Settings >> Signal Contact”).
- Error during selftest.

During a restart, the signal contact is switched off until the mGuard rs4000/rs2000 has started up completely. This also applies when the signal contact is manually set to “Closed” under “Manual settings” in the software configuration.

3.3.4 Antennas

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

NOTE: Removing operator permissions

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

You can find the approved accessories for this wireless system listed with the product at: www.innominate.com.

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

In the case of the **mGuard rs2000 3G**, the WAN is only available via the mobile network, as a WAN interface is not available. The mobile network function is preset. The mGuard rs2000 3G can only be operated in Router mode.

Connecting antennas

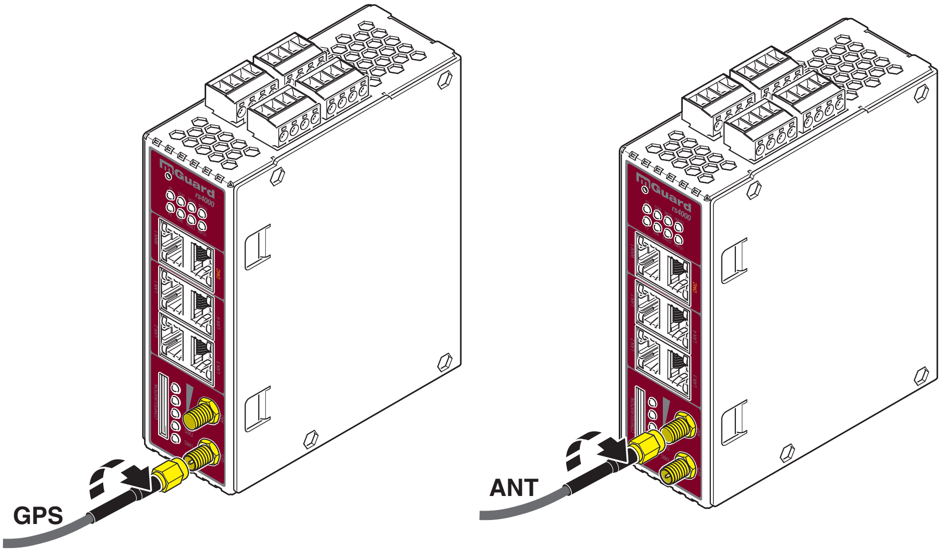


Figure 3-5 Antenna connection

- Connect a suitable antenna to the antenna connection.

  Antenna connection
  - SMA for mobile communication (ANT)
  - RSMA (GPS)
- If the bar graph indicates good or very good reception, affix the antenna (see “Bar graph” on page 53).

3.3.5 SIM card

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

The mGuard rs4000/rs2000 3G can be equipped with two SIM cards. The SIM card in the SIM 1 slot is the primary SIM card which is normally used to establish the connection. If this connection fails, the device can optionally turn to the second SIM card in slot SIM 2. You can set whether, and under which conditions, the connection to the primary SIM card is restored.

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

Quality of the mobile network connection

The signal strength of the mobile network connection is indicated by three LEDs on the front of the mGuard rs4000/rs2000 3G. The LEDs function as a bar graph (refer to “Bar graph” on page 53).

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

Inserting the SIM card

You will receive a SIM card from the wireless provider on which all data and services for your connection are stored. If you use CDMA networks in the USA (e.g., from Verizon Wireless), you will not receive a SIM card. Change the mGuard rs4000/rs2000 3G to a CDMA provider via the web interface.

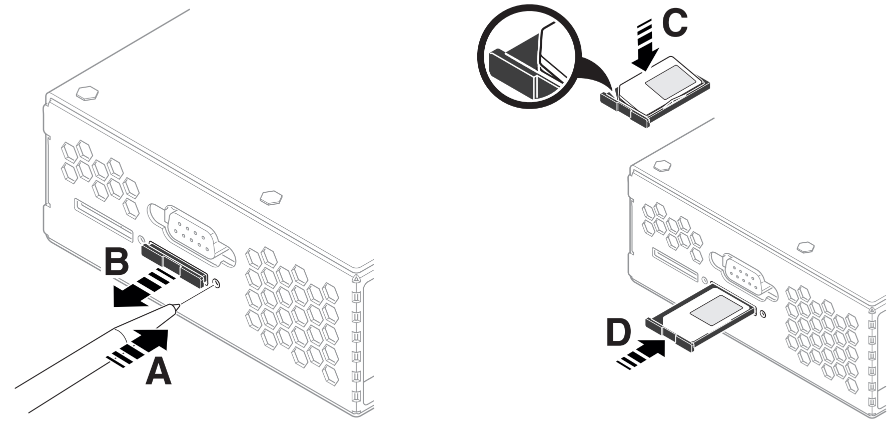


Figure 3-6 Insert the SIM card

To insert the SIM card, proceed as follows:

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

3.3.6 Connecting the supply voltage

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

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

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

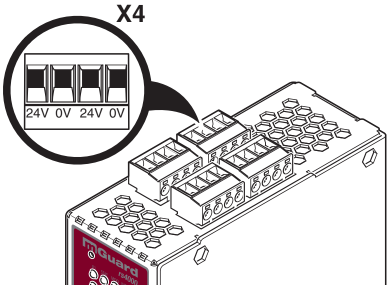
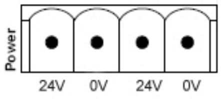
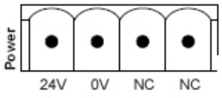


Figure 3-7 Connecting the supply voltage (mGuard rs4000 3G)

Table 3-3 Supply voltage mGuard rs4000/rs2000 3G

mGuard rs4000 3G	mGuard rs2000 3G
	

The mGuard rs4000 3G has a redundant supply voltage. If you only connect one supply voltage, you will get an error message.

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

Status LED P1 lights up green when the supply voltage has been connected properly. On the mGuard rs4000 3G, the status indicator P2 also lights up if there is a redundant supply voltage connection.

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

Redundant voltage supply (mGuard rs4000 3G)

A redundant supply voltage can be connected. Both inputs are isolated. The load is not distributed. With a redundant supply, the power supply unit with the higher output voltage supplies the mGuard rs4000 3G alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the mGuard rs4000 3G indicates the failure of the supply voltage via the signal contact. This message can be prevented by feeding the supply voltage via both inputs or by installing an appropriate wire jumper between the connections.

3.4 Preparing the configuration

3.4.1 Connection requirements

- The **mGuard rs4000/rs2000 3G** must be connected to at least one active power supply unit.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the mGuard.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

3.5 Configuration in Router mode

On initial startup, the mGuard can be accessed via the following address:

- https://192.168.1.1

3.5.1 IP address 192.168.1.1

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

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

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

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

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

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

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

3.6 Establishing a local configuration connection

Web-based administrator interface

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

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

The mGuard can be accessed via the following address:

Table 3-4 Preset address

Default setting	Network mode	Management IP #1
mGuard rs4000 3G	Router	https://192.168.1.1/
mGuard rs2000 3G	Router	https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 3-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 69).

If the administrator web page is not displayed

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

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

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

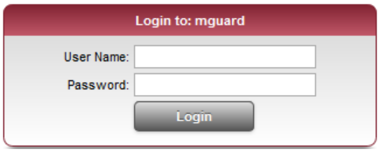


Figure 3-8 Login

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

User Name:	admin
Password:	mGuard

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

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

3.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

Configuration

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

3.8 Restart, recovery procedure, and flashing the firmware

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

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

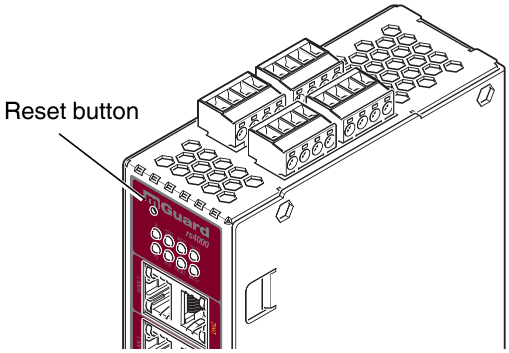


Figure 3-9 Reset button

3.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

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

3.8.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 3-5 Preset address

Default setting	Network mode	Management IP #1
mGuard rs4000 3G	Router	https://192.168.1.1/
mGuard rs2000 3G	Router	https://192.168.1.1/

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

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

Possible reasons for performing the recovery procedure:

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

> Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.
>
> You can find application notes under the following Internet address:
> www.innominate.com.

Action

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

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

3.8.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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

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

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

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

To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 258).

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

– The mGuard firmware has been obtained from your dealer's support team or the www.innominate.com website and has been saved on a compatible SD card.

– This SD card has been inserted into the mGuard.

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

Firmware/install-ubi.mpc83xx.p7s
Firmware/ubifs.img.mpc83xx.p7s

Action

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

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

- Hold down the Reset button until the Stat, Mod, and Sig LEDs light up green. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the rescue system: It searches for a DHCP server via the LAN interface in order to obtain an IP address. (Exception: if an SD card is inserted into the device with corresponding firmware, the rescue system is started from there).

  The Stat LED flashes.

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

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

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

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

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

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

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

- Restart the mGuard. To do so, press the Reset button.

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

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 65):

3.9 Technical data

Hardware properties	mGuard rs4000 3G	mGuard rs2000 3G
Platform	Freescale network processor	Freescale network processor
Network interfaces	4 LAN Ports (managed) ǀ 1 DMZ port ǀ 1 WAN port Ethernet IEEE 802.3 10/100-BaseTX RJ45 ǀ full duplex ǀ auto MDIX	4 LAN ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ45 ǀ full duplex ǀ auto MDIX
Wireless interface	WAN ǀ GSM ǀ GPRS ǀ EDGE ǀ UMTS ǀ CDMA2000	WAN ǀ GSM ǀ GPRS ǀ EDGE ǀ UMTS ǀ CDMA2000
SIM interfaces (1 + 2)	1.8 V ǀ 3 V, redundant	1.8 V ǀ 3 V, redundant
Data rate	≤ 14.4 Mbps (HSDPA)	≤ 14.4 Mbps (HSDPA)
Other interfaces	Serial RS-232 ǀ D-SUB 9 connector 3 digital inputs and 3 digital outputs	Serial RS-232 ǀ D-SUB 9 connector 3 digital inputs and 3 digital outputs
Memory	128 MB RAM ǀ 128 MB Flash ǀ SD card Replaceable configuration memory	128 MB RAM ǀ 128 MB Flash ǀ SD card Replaceable configuration memory
Redundancy options	Optional: VPN ǀ router and firewall	–
Power supply	Voltage range 11 ... 36 V DC, redundant	Voltage range 11 ... 36 V DC, redundant
Power consumption	typical < 200 mA (24 V DC) ǀ maximum < 800 mA (10 V DC)	typical < 200 mA (24 V DC) ǀ maximum < 800 mA (10 V DC)
Humidity range	5% ... 95% (operation, storage), non-condensing	5% ... 95% (operation, storage), non-condensing
Degree of protection	IP20	IP20
Temperature range	-40°C ... +60°C (operation) -40°C ... +70°C (storage)	-40°C ... +60°C (operation) -40°C ... +70°C (storage)
Dimensions (H x W x D)	130 x 45 x 114 mm (up to DIN rail support)	130 x 45 x 114 mm (up to DIN rail support)
Weight	850 g	835 g

Firmware and power values	mGuard rs4000 3G	mGuard rs2000 3G
Firmware compatibility	For mGuard v8.0 or later: Innominate recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.	
Data throughput (router ǀ firewall)	Router mode, default firewall rules, bidirectional throughput: 99 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 50 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	
Virtual Private Network (VPN)	IPsec (IETF standard) Up to 250 VPN tunnels	IPsec (IETF standard) Up to 2 VPN tunnels
Hardware-based encryption	DES ǀ 3DES ǀ AES-128/192/256	DES ǀ 3DES ǀ AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: 35 Mbps, maximum Stealth mode, default firewall rules, bidirectional throughput: 25 Mbps, maximum When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.	
Data throughput (mobile)	Depending on the mobile connection ≤ 14,4 Mbit/s (HSDPA) upload ≤ 5,7 Mbit/s (HSDPA) download	
Management support	Web GUI (HTTPS) ǀ command line interface (SSH) ǀ SNMP v1/2/3 ǀ central device management software	
Diagnostics	13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signal Status, SIM Status) ǀ Service I/Oǀ Log File ǀ Remote Syslog	

Other	mGuard rs4000 3G	mGuard rs2000 3G
Conformance	CE I FCC I UL 508 I electrical isolation (VCC//PE) I ANSI / ISA 12.12 Class I Div. 2	
Special features	GPS / GLONASS receiver I realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Secure Cloud ready	

4 mGuard delta^2

Table 4-1 Available mGuard delta^2 versions

Available versions	Order No.
mGuard delta^2 TX/TX	HW-103060
mGuard delta^2 TX/TX VPN	BD-211010

The **mGuard delta^2** is ideal for use in desktop applications, in distribution compartments, and other environments close to production processes with low requirements for industrial hardening.

Individual devices or network segments can be safely networked and comprehensively protected. The mGuard delta^2 can be used as a firewall between office and production networks as well as a security router for small and medium-sized workgroups.

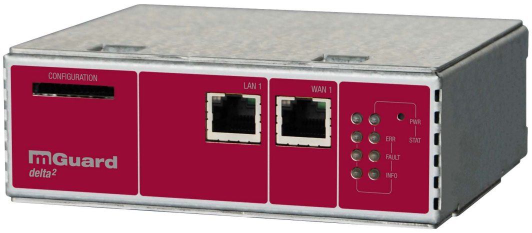


Figure 4-1 mGuard delta^2

4.1 Operating elements and LEDs

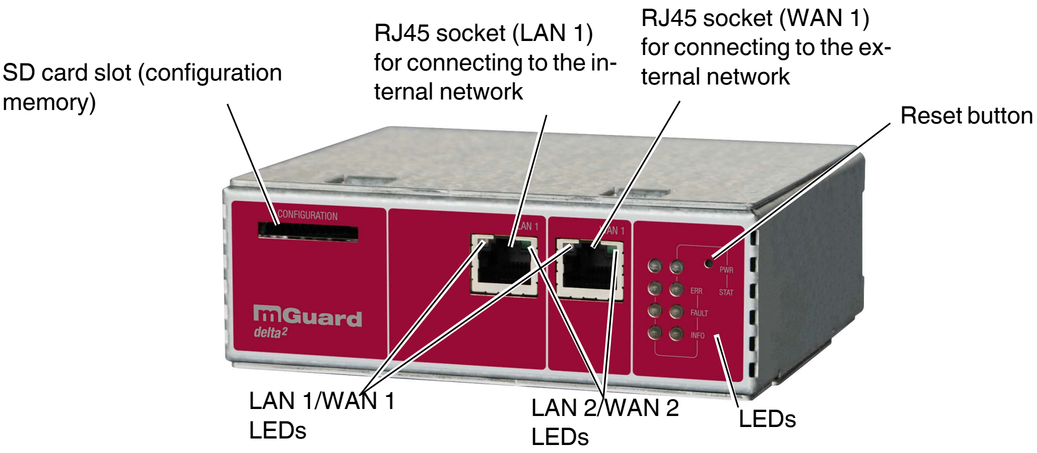

SD card slot (configuration memory)
RJ45 socket (LAN 1) for connecting to the internal network
RJ45 socket (WAN 1) for connecting to the external network
Reset button
CONFIGURATION
LAN 1
WAN 1
PWR
ERR
STAT
FAULT
INFO
mGuard
delta^2
LAN 1/WAN 1 LEDs
LAN 2/WAN 2 LEDs
LEDs

Figure 4-2 Operating elements and LEDs on the

Table 4-2 LEDs on the mGuard delta^2

LEDs	State		Meaning
WAN 1 **LAN 1**	Green	On	Full duplex
		Off	Half duplex
WAN 2 **LAN 2**	Yellow	On	10 Mbps
		Flashing	10 Mbps, data transmission active
	Green	On	100 Mbps
		Flashing	100 Mbps, data transmission active
PWR	Green	On	Supply voltage OK
STAT	Green	Flashing	The mGuard is ready to operate.
ERR	Red	On	System error
FAULT	Red	On	mGuard in the booting or flashing state
INFO			Not used

4.2 Startup

4.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:

  0°C ... +40°C

- Maximum humidity, non-condensing:

  5% ... 95%

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

NOTE: Cleaning

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

4.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard delta^2
- Package slip
- 12 V DC power supply including different country adapters

4.3 Connecting the mGuard delta^2

NOTE: Notes on mounting and installation

Only connect the RJ45 Ethernet ports of the mGuard to matching network installations. Some telecommunications connections also use RJ45 sockets. You may not connect these to the RJ45 ports of the mGuard.

Safe isolation of live circuits is only guaranteed if connected devices fulfill requirements specified by VDE 0106-101 (safe isolation). The supply lines must be isolated or laid separately to live circuits.

4.3.1 Connecting to the network

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

4.3.2 Connecting the supply voltage

- Connect the wide-range power supply unit of the mGuard to a suitable power supply. Connect the low-voltage plug of the power supply unit on the back of the mGuard.

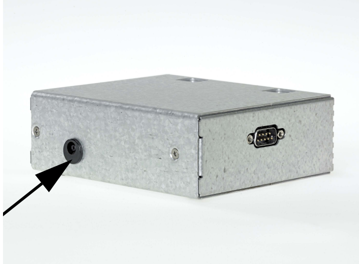


Figure 4-3 Low-voltage plug of the power supply unit

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

The mGuard boots the firmware. Status LED STAT flashes green.

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

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

4.4 Preparing the configuration

4.4.1 Connection requirements

mGuard delta^2

- The mGuard delta^2 must be connected to its power supply.
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the mGuard.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

4.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 4-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard delta^2	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (in the web interface under “Network >> Interfaces >> General”). Alternatively, you can select a different stealth configuration or use another network mode.

4.5 Configuration in Stealth mode

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

- https://192.168.1.1/ (see Page 81)
- https://1.1.1.1/ (see Page 81)

Alternatively, an IP address can be assigned via BootP (see "Assigning the IP address via BootP" on page 82).

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

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

4.5.1 IP address 192.168.1.1

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

– The mGuard is in the delivery state.

– The mGuard was reset to the default settings via the web interface and restarted.

– The rescue procedure (flashing of the mGuard) or the recovery procedure has been performed.

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

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

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

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

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

4.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the 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 and if the default gateway can be accessed via the WAN port of the mGuard at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 83). 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

4.5.3 Assigning the IP address via BootP

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

For IP address assignment, the 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.

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

Notes for BootP

During initial startup, the mGuard transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the mGuard no longer sends BootP requests. The FL MGUARD can then no longer be accessed via IP address 192.168.1.1.

After receiving a BootP reply, the mGuard no longer sends BootP requests, not even after it has been restarted. For the 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 mGuard is connected to a computer using a Microsoft Windows operating system.

4.6 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 4-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard delta^2	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

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

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

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

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 87).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 79).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

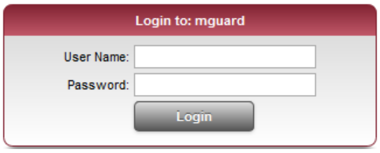


Figure 4-4 Login

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

User Name:	admin
Password:	mGuard

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

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

4.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

Configuration

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

4.8 Restart, recovery procedure, and flashing the firmware

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

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

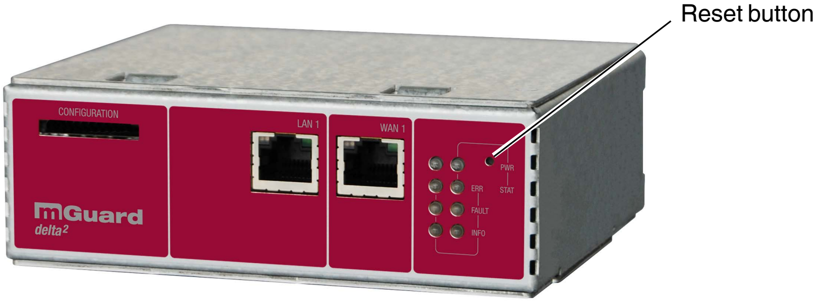


Figure 4-5 Reset button

4.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

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

4.8.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 4-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard delta^2	Stealth	https://1.1.1.1/	https://192.168.1.1/

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

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

Possible reasons for performing the recovery procedure:

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

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

4.8.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

> **NOTE:** During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.
>
> The following requirements apply when loading the firmware from an SD card:
>
> - All necessary firmware files must be located in a common directory on the first partition of the SD card.
> - This partition must use a VFAT file system (standard type for SD cards).
>
> To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 258).

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

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

  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s

Action

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

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

- Hold down the Reset button until the STAT, MOD, and SIG LEDs light up green. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The STAT LED flashes.

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

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

  The STAT, MOD, and SIG LEDs form a running light.

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

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

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

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

- Restart the mGuard. To do this, briefly press the Reset button.

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

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 83):

4.9 Technical data

Hardware properties	
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232, D-SUB 9 connector
Memory	128 MB RAM I 128 MB Flash SD card, replaceable configuration memory
Redundancy options	Optional: VPN I router
Power supply	External power supply unit 12 V/0.85 A DC I 100 – 240 V/0.4 A AC
Power consumption	2.13 W, typical
Humidity range	5% ... 95% during operation, non-condensing
Degree of protection	IP20
Temperature range	0°C ... +40°C (operation) 0°C ... +60°C (storage)
Dimensions (H x W x D)	45 x 130 x 114 mm
Weight	629 g

Firmware and power values	
Firmware compatibility	For mGuard v7.4.0 or later: Innominate recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	Router mode, default firewall rules, bidirectional throughput: max. 99 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 50 Mbps
Virtual Private Network (VPN)	IPsec (IETF standard), VPN models up to 10 tunnels, Optionally up to 250 VPN tunnels
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: max. 35 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 25 Mbps
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (Power, State, Error, Signal, Fault, Info) I log file I remote syslog

Other	
Conformance	CE I FCC
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Remote Services Portal ready

5 mGuard pci^2 SD

Table 5-1 Available mGuard pci^2 SD versions

Available versions	Order No.
mGuard pci^2 SD	HW-102061
mGuard pcie^2 SD	HW-102071
mGuard pci^2 SD VPN	BD-111040
mGuard pcie^2 SD VPN	BD-111060

The **mGuard pci^2 SD** has the design of a PCI-compatible plug-in board. It is available in two versions:

- **mGuard pci^2 SD** for devices or machines with PCI bus
- **mGuard pcie^2 SD** for devices or machines with PCI Express bus

To aid understanding, mGuard pci^2 SD is used for the two device versions in this user manual.

The mGuard pci^2 SD is suitable for distributed protection of industrial and panel PCs, individual machines or industrial robots. It has a configuration memory in the form of a replaceable SD card, which can be easily accessed on the front.

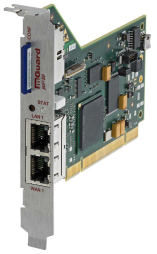


Figure 5-1 mGuard pci^2 SD

5.1 Operating elements and LEDs

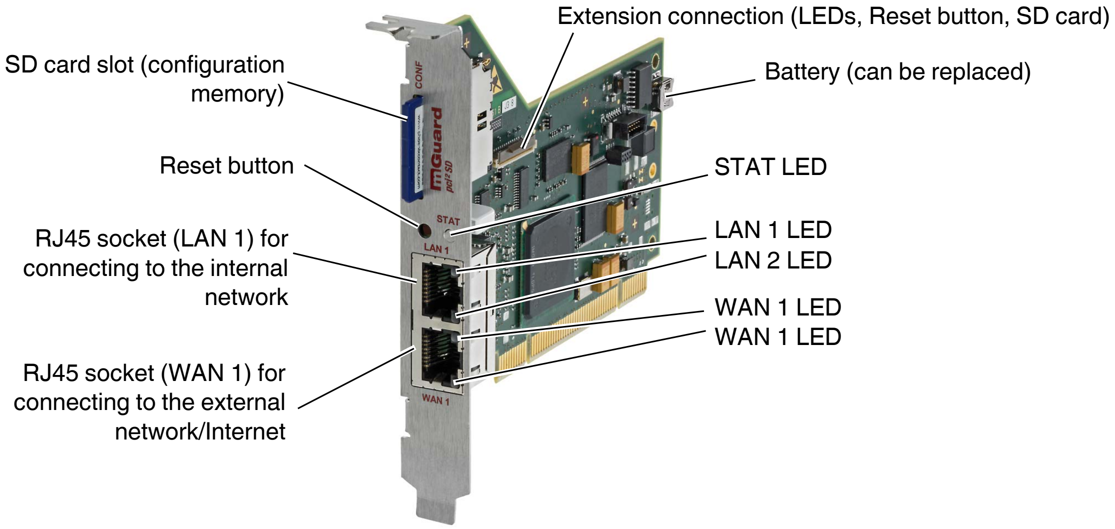

Extension connection (LEDs, Reset button, SD card)
SD card slot (configuration memory)
Battery (can be replaced)
Reset button
STAT LED
RJ45 socket (LAN 1) for connecting to the internal network
LAN 1 LED
LAN 2 LED
WAN 1 LED
WAN 1 LED
RJ45 socket (WAN 1) for connecting to the external network/Internet
CONF
mGuard
pci² SD
STAT
LAN 1
WAN 1

Figure 5-2 Operating elements and LEDs on the mGuard pci^2 SD

Table 5-2 LEDs on the mGuard pci^2 SD

LEDs	State		Meaning
WAN 1 **LAN 1**	Green	On	Full duplex
		Off	Half duplex
WAN 2 **LAN 2**	Yellow	On	10 Mbps
		Flashing	10 Mbps, data transmission active
	Green	On	100 Mbps
		Flashing	100 Mbps, data transmission active
LAN 1 **LAN 2** **WAN 1**	Various LED light codes		**Recovery procedure/flashing** See “Restart, recovery procedure, and flashing the firmware” on page 104.
STAT	Red/green	Flashing	**Boot process.** When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
	Green	Flashing	**Heartbeat**. The mGuard is connected correctly and ready to operate.
	Red	Flashing	**System error**. Restart the device. • Press the Reset button (for 1.5 seconds). • Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see “Performing a recovery procedure” on page 105) or contact your dealer.

5.2 Startup

5.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

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 mGuard pci^2 SD.
- Do not bend connecting cables. Only use the network plug for connection to a network.

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C ... +60°C (mGuard pci^2 SD with battery)
  0°C ... +70°C (mGuard pci^2 SD without battery)
- Maximum humidity, non-condensing:
  5% ... 95%

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

NOTE: Cleaning

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

5.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard pci^2 SD
- Package slip

5.3 Installation of mGuard pci^2 SD

WARNING: This is a Class A item of equipment. This equipment can cause radio interference in residential areas; in this case, the operator may be required to implement appropriate measures.

WARNING: Safe isolation of live circuits is only guaranteed if connected devices fulfill requirements specified by VDE 0106-101 (safe isolation). The supply lines must be isolated or laid separately to live circuits.

5.3.1 Installing the hardware

NOTE: Electrostatic discharge

Before installation, touch the metal frame of the PC in which the mGuard pci^2 SD is to be installed, in order to remove electrostatic discharge.

The device contains components that can be damaged or destroyed by electrostatic discharge. When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) according to EN 61340-5-1 and IEC 61340-5-1.

mGuard pci^2 SD: structure

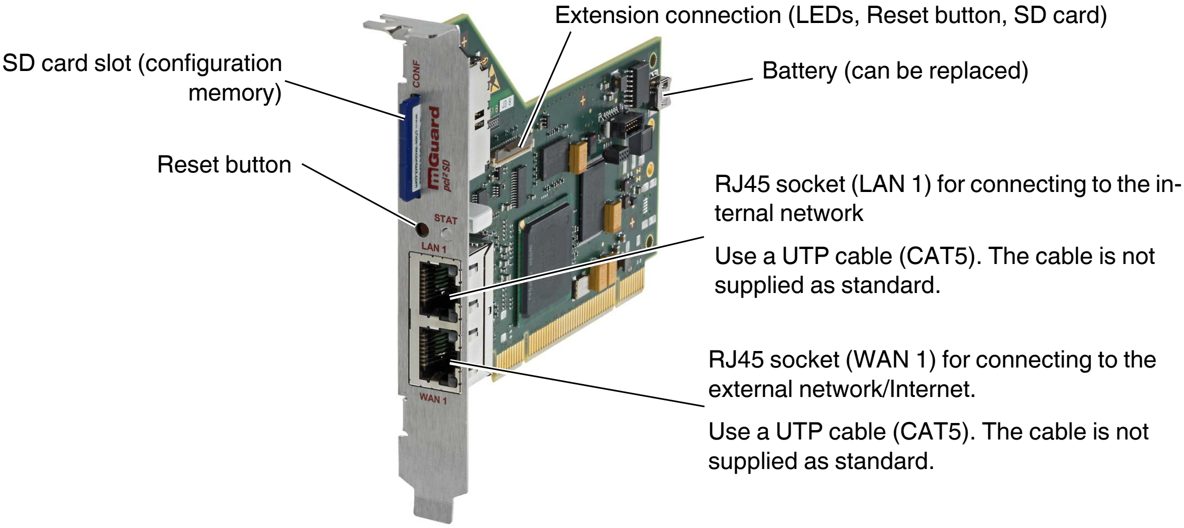

Extension connection (LEDs, Reset button, SD card)
SD card slot (configuration memory)
Battery (can be replaced)
Reset button
RJ45 socket (LAN 1) for connecting to the internal network
Use a UTP cable (CAT5). The cable is not supplied as standard.
RJ45 socket (WAN 1) for connecting to the external network/Internet.
Use a UTP cable (CAT5). The cable is not supplied as standard.
CONF
mGuard
pci² SD
STAT
LAN 1
WAN 1

Figure 5-3 mGuard pci^2 SD structure

- Install the mGuard pci^2 SD in a free PCI or PCI Express slot. Observe the notes in the documentation for your system.

5.4 Preparing the configuration

5.4.1 Connection requirements

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

5.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 5-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard pci^2 SD	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 101). Alternatively, you can select a different stealth configuration or use another network mode.

5.5 Configuration in Stealth mode

The mGuard pci^2 SD can be started up in three different ways:

- Start up the device in Stealth mode (standard)
- Start up the device via temporary management IP address
- Start up device via BootP

5.5.1 Start up the device in Stealth mode (standard)

Insert the mGuard pci^2 SD between an existing network connection.

To connect to the LAN and WAN interfaces, a suitable UTP cable (CAT5) is required. The cables are not supplied as standard.

- Connect the internal network interface (LAN 1) of the mGuard pci^2 SD to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network.
- Connect the external network interface (WAN 1) of the mGuard pci^2 SD to the external network, e.g., Internet.

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

The mGuard boots the firmware. The STAT status LED flashes green during this time.

The mGuard is ready for operation as soon as the lower Ethernet socket LEDs light up. In addition, the STAT status LED flashes green at heartbeat.

> If the lower LEDs in the Ethernet sockets do not light up, this indicates a missing connection to the internal or external network. If no LED lights up, the supply voltage is missing.

The mGuard is configured via a web browser that is executed on the locally connected computer.

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

The mGuard is preset and can be accessed via address https://1.1.1.1/

Configuring the mGuard pci^2 SD

- Enter the following address into the browser: https://1.1.1.1/

The connection to the mGuard pci^2 SD is established. (If not, see Section 5.5.2).

A security message indicating a possible invalid/not trusted certificate is displayed. This message results from the use of an mGuard certificate from Innominate that is not yet known to the browser but necessary for encryption of the communication.

- Acknowledge this message with “Accept this certificate always/temporarily” (Mozilla Firefox), “Continue loading this website” (Internet Explorer), “Continue anyway” (Google Chrome).
- Click “Yes” to acknowledge the security alert.

The login window is displayed.

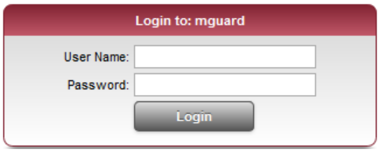


Figure 5-4 Login

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

User Name:	admin
Password:	mGuard

To configure the device, make the desired or necessary settings on the individual pages of the mGuard web interface.

> For security reasons, we recommend you change the default root and administrator passwords during initial configuration (in the web interface under “Authentication >> Administrative Users”).

5.5.2 Starting up the mGuard pci^2 SD via a temporary management IP address

If the mGuard pci^2 SD is connected without a functioning external network in initial startup mode, the device **cannot** be accessed via address https://1.1.1.1/.

In this case, the mGuard pci^2 SD is accessible automatically via management IP address 192.168.1.1/24. This applies to the internal (LAN 1) and the external (WAN 1) network interfaces. An address conflict with the external network interface is not possible as long as WAN 1 is not connected to a functioning network. This management IP address is normally non-persistent.

However, if the external network interface (WAN 1) is connected after booting the mGuard pci^2 SD, the management IP address remains valid. In this case, an address conflict with an existing address in the external network is possible.

Starting up the mGuard pci^2 SD without external network

- Connect the internal network interface (LAN 1) of the mGuard pci^2 SD to the corresponding Ethernet network card of the configuration computer or a valid network connection of the internal network.
- Disconnect the external network interface (WAN 1) of the mGuard pci^2 SD from the external network (WAN).
- Switch on the system. The STAT LED lights up green when the supply voltage has been connected properly.

The mGuard boots the firmware. The STAT LED flashes green.

Adapting the configuration computer

In order to access the mGuard pci^2 for configuration, the configuration computer must be adapted to the management IP address of the mGuard pci^2 SD.

Example of Microsoft Windows XP:

- Set the following in the “Internet Protocol (TCP/IP) Properties” of the relevant network interface of the configuration computer:

IP address:	192.168.1.10
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.2

- Enter the address assigned into the browser: https://192.168.1.1/
- Configure the mGuard as described in “Configuring the mGuard pci^2 SD” on page 97.

5.5.3 Starting up mGuard pci^2 SD via BootP

In initial startup mode, the mGuard pci^2 additionally starts a BootP client on the internal network interface (LAN 1). The BootP client is compatible with the “IPAssign” BootP servers from Phoenix Contact as well as “DHCPD” under Linux.

This software can either be downloaded free of charge at phoenixcontact.net/products or at www.innominate.com under "Downloads > Software".

ℹ IP address assignment using IPAssign is described in detail in “Assigning the IP address using IPAssign.exe” on page 255.

If an non-configured mGuard pci^2 SD accesses a BootP server after booting, the BootP protocol assigns an IP address, a subnet mask, and optionally a default gateway of the internal network interface to the mGuard pci^2 SD. These parameters are saved in the device which can then be immediately accessed under these parameters.

- Enter the address assigned via BootP in the browser: e.g., https://192.168.1.1/

Configure the mGuard as described in “Configuring the mGuard pci^2 SD” on page 97.

5.5.4 Assigning the IP address via BootP

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

For IP address assignment, the 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.

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

Notes for BootP

During initial startup, the mGuard transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the mGuard no longer sends BootP requests. The product can then no longer be accessed via IP address 192.168.1.1.

After receiving a BootP reply, the mGuard no longer sends BootP requests, not even after it has been restarted. For the 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 mGuard is connected to a computer using a Microsoft Windows operating system.

5.6 Establishing a local configuration connection

Web-based administrator interface

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

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

The mGuard can be accessed via the following address:

Table 5-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard pci^2 SD	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

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

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

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

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 105).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 95).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

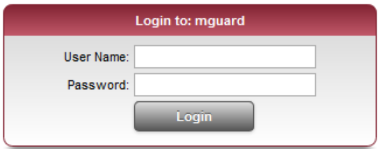


Figure 5-5 Login

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

User Name:	admin
Password:	mGuard

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

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

5.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

Configuration

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

5.8 Restart, recovery procedure, and flashing the firmware

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

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

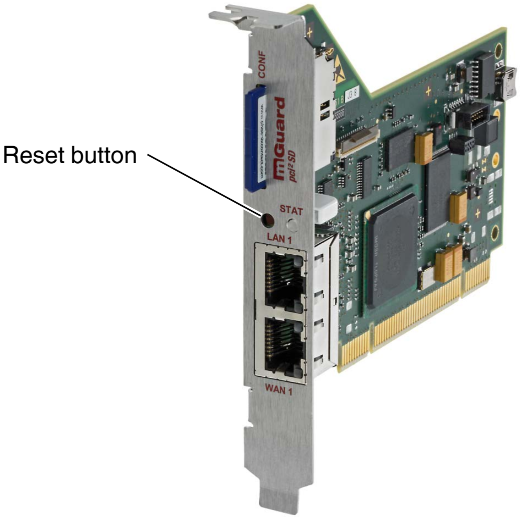


Figure 5-6 Reset button

5.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button until the STAT LED lights up orange.
- Alternatively, restart the computer that contains the mGuard pci card.

5.8.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 5-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard pci^2 SD	Stealth	https://1.1.1.1/	https://192.168.1.1/

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

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

Possible reasons for performing the recovery procedure:

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

> Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.
>
> You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

5.8.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

> **NOTE:** During flashing, the firmware is always loaded from an SD card first. The firmware is only loaded from a TFTP server if no SD card is found.
>
> The following requirements apply when loading the firmware from an SD card:
>
> - All necessary firmware files must be located in a common directory on the first partition of the SD card.
> - This partition must use a VFAT file system (standard type for SD cards).
>
> To flash the firmware from a TFTP server, a TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 258).

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

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

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

- All necessary firmware files must be located in a common directory on the first partition of the SD card.
- This partition must use a VFAT file system (standard type for SD cards).
- The mGuard firmware has been obtained from your dealer's support team or the www.innominate.com website and has been saved on a compatible SD card.
- This SD card has been inserted into the mGuard.
- The relevant firmware files are available for download from the download page of www.innominate.com. The files must be located under the following path names or in the following folders on the SD card:

  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s

Action

- Press and hold down the Reset button on the front plate.

  The STAT LED on the front plate briefly lights up orange.
  Then the STAT LED and the upper two LEDs of the Ethernet sockets light up green one after the other.
- Release the Reset button during the green light phase.

  The flashing procedure is started.

5.9 Technical data

mGuard pci^2 SD | mGuard pcie^2 SD

Hardware properties		
Platform		Freescale network processor with 330 MHz clocking
Network interfaces		1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ45 I full duplex I auto MDIX
Other interfaces		Serial RS-232, internal connector
Memory		128 MB RAM I 128 MB Flash SD card I replaceable configuration memory
Drives		–
Redundancy options		Optional: VPN I router
Power supply		3.3 V or 5 V via PCI (mGuard pci^2 SD) or PCI Express bus (mGuard pcie^2 SD)
Power consumption		Typical, 3.7 W ... 4.2 W
Humidity range		5% ... 95% during operation and storage, non-condensing
Degree of protection		Depending on installation type and on the host system
Temperature range	Without battery (HT version)	0°C ... +70°C (operation) -20°C ... +70°C (storage)
	With battery	0°C ... +60°C (operation) -20°C ... +60°C (storage)
Dimensions (H x W x D)		950 mm X 18 mm X 130 mm
Weight		72 g

Firmware and power values	
Firmware compatibility	For mGuard v7.5.0 or later: Innominate recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	Router mode, default firewall rules, bidirectional throughput: max. 99 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 50 Mbps
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: max. 35 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 25 Mbps
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (2 x LAN, 2 x WAN in combination) for Ethernet status and speed; 1 LED for Power, Error, State, Fault, Info) I log file I remote-syslog

Other	
Conformance	CE I FCC
Special features	Realtime clock I Trusted Platform Module (TPM) I temperature sensor I mGuard Remote Services Portal ready

6 mGuard smart^2/smart

Table 6-1 Available mGuard smart^2 / mGuard smart versions

Available versions	Order No.
mGuard smart^2	HW-101130
mGuard smart^2 VPN	BD-101030
mGuard smart / 266	HW-101020
mGuard smart / 533	HW-101050
mGuard smart / 266 VPN	BD-101010
mGuard smart / 533 VPN	BD-101020

The **mGuard smart^2** is the smallest device version. For example, it can be inserted between the computer or local network and an available router, without having to make configuration changes or perform driver installations on the existing system. It is designed for instant use in the office or when traveling.

The mGuard smart^2 is a further development of the **mGuard smart**. To aid understanding, mGuard smart^2 is mostly used for the two device versions in this user manual. The properties described also apply to the mGuard smart. Differences from the mGuard smart are indicated, if applicable.

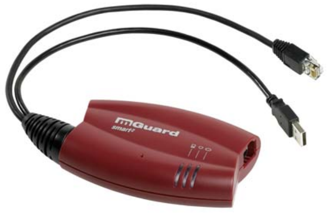


Figure 6-1 mGuard smart^2

6.1 Operating elements and LEDs

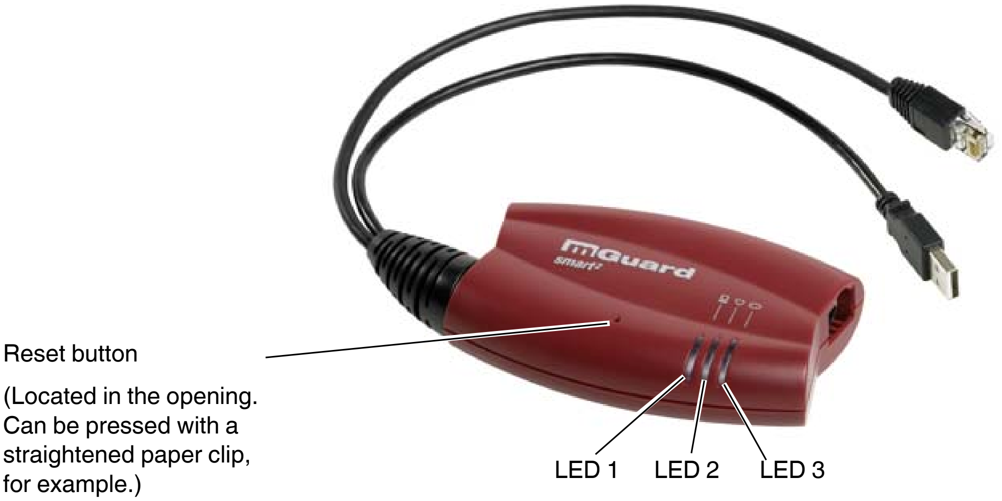

Reset button
(Located in the opening. Can be pressed with a straightened paper clip, for example.)
LED 1
LED 2
LED 3

Figure 6-2 Operating elements and LEDs on the mGuard smart^2

Table 6-2 LEDs on the mGuard smart^2

LED	State		Meaning
1	Green	On	LAN: connection to the network partner is present
		Flashing	LAN: data transmission is active
2	Red/gree n	Flashing	**Boot process**. When the device has just been connected to the power supply. After a few seconds, this LED changes to the heartbeat state.
	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
	Red	Flashing	**System error**. Restart the device. • Press the Reset button (for 1.5 seconds). • Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see “Performing a recovery procedure” on page 121) or contact your dealer.
3	Green	On	WAN: connection to the network partner is present
		Flashing	WAN: data transmission is active
1, 2, 3	Various LED light codes		**Recovery mode**. After pressing the **Reset button**. See “Restart, recovery procedure, and flashing the firmware” on page 120.

6.2 Startup

6.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C ... +40°C
- Maximum humidity, non-condensing
  20% ... 90%

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

NOTE: Cleaning

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

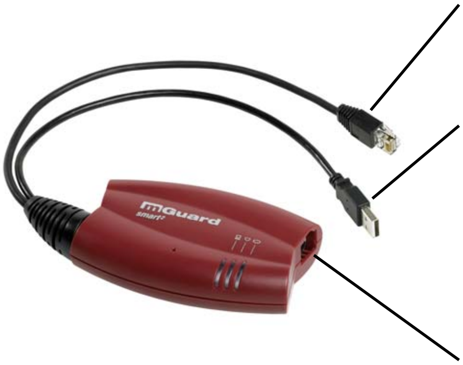
6.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard smart^2
- Package slip

6.3 Connecting the mGuard smart^2



LAN port

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

USB plug

For connection to the USB interface of a computer.

For the power supply (default settings).

The mGuard smart^2 (not the mGuard smart) can be configured so that a serial console is available via the USB plug.

WAN port

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

Use a UTP cable (CAT5).

Before:

After:

(A LAN can also be on the left.)

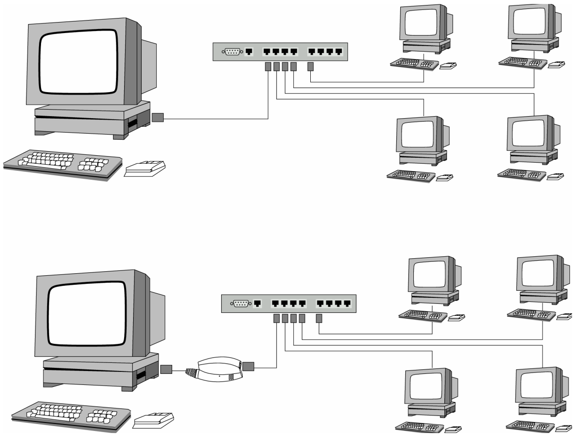


Figure 6-3 mGuard smart^2: Connection in the network

If your computer is already connected to a network, insert the mGuard smart^2 between the network interface of the computer (i.e., its network card) and the network.

Driver installation is not required.

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

WARNING: This is a Class A item of equipment. This equipment can cause radio interference in residential areas; in this case, the operator may be required to implement appropriate measures.

6.4 Preparing the configuration

6.4.1 Connection requirements

- The mGuard smart^2 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 mGuard
  - Or must be connected to the mGuard via the local network
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

6.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 6-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard smart^2	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 117). Alternatively, you can select a different stealth configuration or use another network mode.

6.5 Configuration in Stealth mode

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

- https://192.168.1.1/ (see Page 115)
- https://1.1.1.1/ (see Page 115)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 116).

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

Computers can access the mGuard via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the mGuard. For this purpose, the 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 product can no longer be accessed via IP address 192.168.1.1.

6.5.1 IP address 192.168.1.1

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

– The mGuard is in the delivery state.

– The mGuard was reset to the default settings via the web interface and restarted.

– The rescue procedure (flashing of the mGuard) or the recovery procedure has been performed.

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

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

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

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

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

6.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the 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 and if the default gateway can be accessed via the WAN port of the mGuard at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 117). Continue from this point.

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

6.5.3 Assigning the IP address via BootP

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

For IP address assignment, the 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.

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

Notes for BootP

During initial startup, the mGuard transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the mGuard no longer sends BootP requests. The product can then no longer be accessed via IP address 192.168.1.1.

After receiving a BootP reply, the mGuard no longer sends BootP requests, not even after it has been restarted. For the 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 mGuard is connected to a computer using a Microsoft Windows operating system.

6.6 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 6-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard smart^2	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network setting”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 6-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 121).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 113).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.
  Click on “Properties” under “LAN settings”.
  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

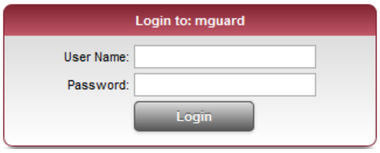


Figure 6-4 Login

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

User Name:	admin
Password:	mGuard

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

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

6.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

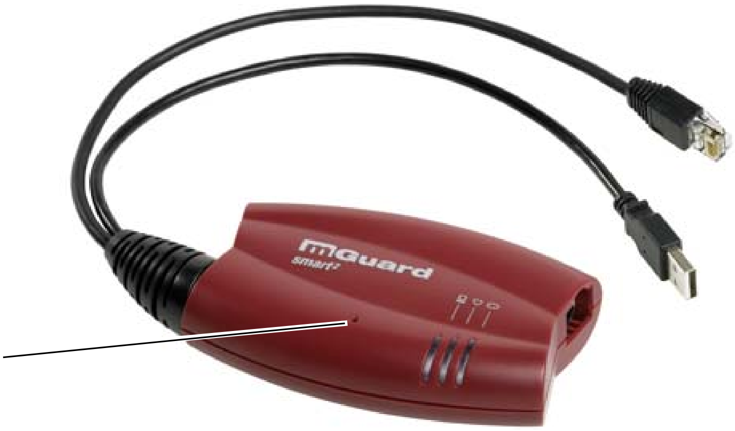
Configuration

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

6.8 Restart, recovery procedure, and flashing the firmware

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

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



Reset button

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

Figure 6-5 Reset button

6.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the middle LED lights up in red.
  (Alternatively, you can disconnect and insert the USB cable, as it is only used for the power supply.)

6.8.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 6-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard smart^2	Stealth	https://1.1.1.1/	https://192.168.1.1/

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

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

Possible reasons for performing the recovery procedure:

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

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

6.8.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

> **NOTE:** To flash the firmware, a DHCP and TFTP server or a BootP and TFTP server must be installed on the locally connected computer.
>
> Install the DHCP and TFTP server, if necessary (see “Installing the DHCP and TFTP server” on page 258).

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

Action

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

- Hold down the Reset button until the LEDs light up green. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The middle LED flashes.

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

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

  The three green LEDs form a running light.

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

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

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.
- As soon as the procedure is complete, all LEDs flash green simultaneously.
- Restart the mGuard. To do this, briefly press the **Reset button**.

  Alternatively, you can disconnect and insert the USB cable, as it is only used for the power supply.

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 117):

6.9 Technical data

mGuard smart^2

Hardware properties	
Platform	Freescale network processor with 330 MHz clocking
Network interfaces	1 LAN port ǀ 1 WAN port Ethernet IEEE 802.3 10/100 Base TX ǀ RJ45 ǀ full duplex ǀ auto MDIX
Other interfaces	Serial via USB connection
Drives	–
Redundancy options	Depending on the firmware used
Power supply	Via USB interface (5 V at 500 mA) Optional: external power supply unit (110 V ... 230 V)
Power consumption	2.5 W, maximum
Temperature range	0°C ... +40°C (operation) -20°C ... +60°C (storage)
Humidity range	20% ... 90% during operation, non-condensing
Degree of protection	IP30
Dimensions (H x W x D)	27 x 77 x 115 mm
Weight	131 g

Firmware and power values	
Firmware compatibility	For mGuard v7.2 or later: Innominate recommends the use of the latest firmware version and patch releases in each case. For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router ǀ firewall)	Router mode, default firewall rules, bidirectional throughput: max. 99 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 50 Mbps
Hardware-based encryption	DES ǀ 3DES ǀ AES-128/192/256
Encrypted VPN throughput (AES-256)	Router mode, default firewall rules, bidirectional throughput: max. 35 Mbps Stealth mode, default firewall rules, bidirectional throughput: max. 25 Mbps
Management support	Web GUI (HTTPS) ǀ command line interface (SSH) ǀ SNMP v1/2/3 ǀ central device management software
Diagnostics	3 LEDs (in combination for boot process, heartbeat, system error, Ethernet status, Recovery mode) ǀ Log File ǀ Remote Syslog

Other	
Conformance	CE ǀ FCC
Special features	Realtime clock ǀ Trusted Platform Module (TPM) ǀ temperature sensor

6.9.1 mGuard smart

mGuard smart /266 | mGuard smart /533

Hardware properties	
Platform	Intel network processor either with 533 MHz or 266 MHz clocking
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100 Base TX I RJ45 I full duplex I auto MDIX
Other interfaces	–
Drives	–
Redundancy options	Depending on the firmware used
Power supply	Via USB interface (5 V at 500 mA) Optional: external power supply unit (110 V ... 230 V)
Power consumption	2.5 W, maximum
Temperature range	0°C ... +40°C (operation) -20°C ... +70°C (storage)
Humidity range	20% ... 90% during operation, non-condensing
Degree of protection	IP30
Dimensions (H x W x D)	27 x 77 x 115 mm
Weight	158 g

Firmware and power values	
Firmware compatibility	mGuard v5.0 or later: Innominate recommends firmware version 6.x or 7.x to be used with the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	99 Mbps bidirectional I 99 Mbps bidirectional
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	35 Mbps (smart/256) bidirectional I 70 Mbps (smart/533) 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 I FCC

7 mGuard centerport^2

Table 7-1 Available mGuard centerport^2 versions

Available versions	Order No.
mGuard centerport^2	HW-106010
mGuard centerport^2 VPN 250	BD-621000
mGuard centerport^2 VPN 1000	BD-622000

The **mGuard centerport^2** is a high-end firewall and a VPN gateway in 19" format. It is suitable as a central network infrastructure for remote service solutions. With its Gigabit Ethernet interfaces and corresponding throughput as the router and as the stateful inspection firewall, the device can also be used in the backbone in industrial networks.

As a gateway, the mGuard centerport^2 supports the VPN connection to any number of systems in the VPN tunnel groups with up to three thousand simultaneously active tunnels, which all belong to the same unique public IP address.

The mGuard centerport^2 performs secure remote services, such as remote support, remote diagnostics, remote maintenance, and condition monitoring for a large number of machines and systems via the Internet. An encrypted VPN data throughput of 600 Mbps is possible at one interface.

The mGuard centerport^2 is compatible with all mGuard field devices and the mGuard device manager.

The mGuard centerport^2 can be provided in three device versions, which determine the number of simultaneously supported active VPN tunnels: mGuard centerport^2, mGuard centerport^2 VPN-250, mGuard centerport^2 VPN-1000. VPN licenses can be installed later, if required.

Figure 7-1 mGuard centerport^2

7.1 Operating elements and LEDs

Front

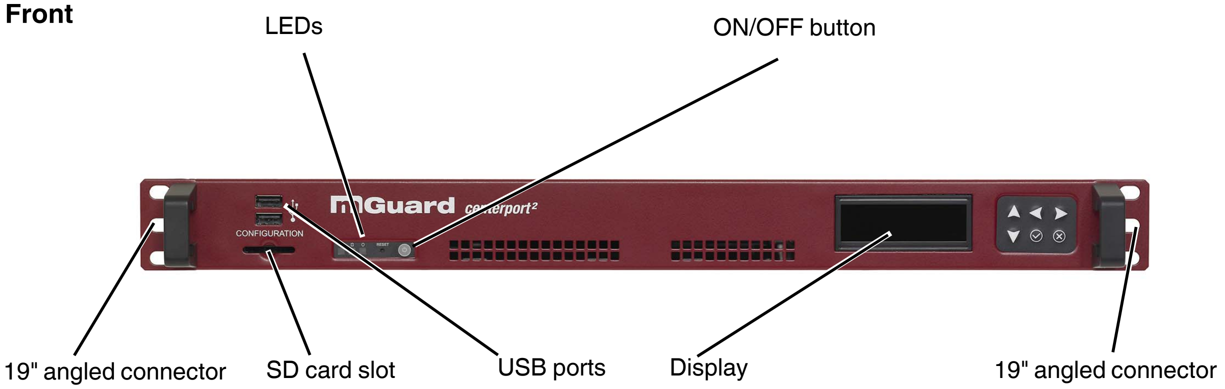


Figure 7-2 Operating elements and LEDs on the mGuard centerport² front side

Table 7-2 LEDs on the mGuard centerport²

LED	State	Meaning
Green	On	Lights up if the system is switched on
Orange	On	Lights up while hard disk is accessed

7.2 Startup

7.2.1 Safety notes

Personnel

Installation, startup and maintenance of the product may only be performed by qualified specialist personnel who have been authorized for this by the operator. Specialist personnel must have read and understood the instructions in this manual and act accordingly.

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C ... +45°C
- Maximum humidity, non-condensing:
  20% ... 90%

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

NOTE: Risk of material damage caused by cleaning agents

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

7.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard centerport²
- Package slip
- 2 x AC mains connecting cables
- 19'' server rails/telescopic rails (2 x short, 2 x long)
- Screw set
- Installation instructions for 19'' frame/industrial cabinet (Quickrails installation instructions)

7.3 Installing and booting the mGuard centerport^2

Back

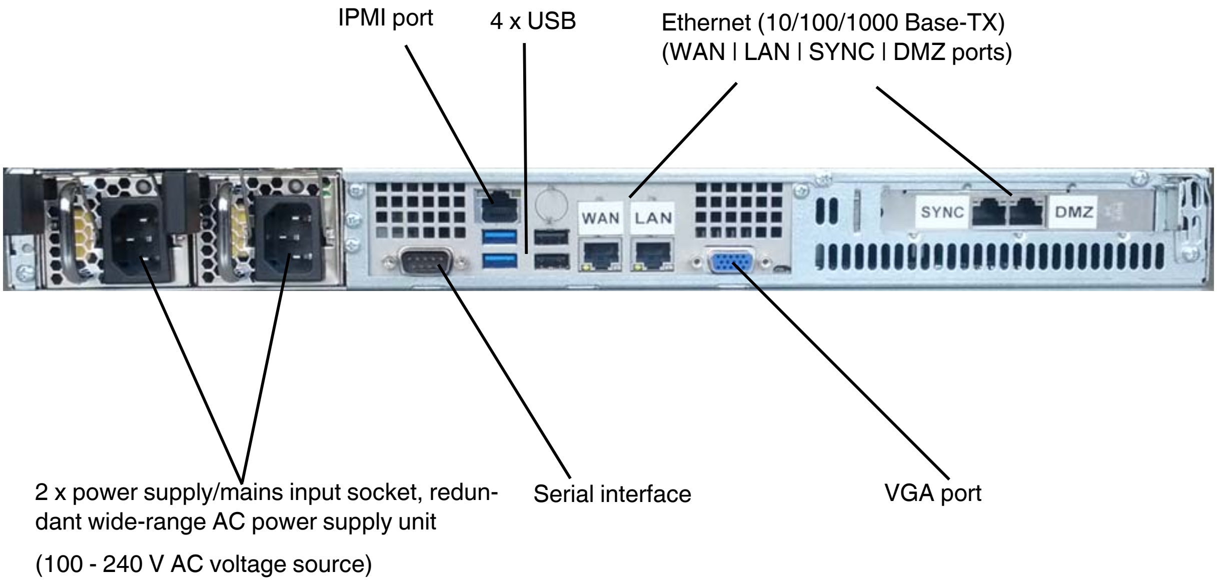

IPMI port
4 x USB
Ethernet (10/100/1000 Base-TX)
(WAN I LAN I SYNC I DMZ ports)
WAN
LAN
SYNC
DMZ
2 x power supply/mains input socket, redundant wide-range AC power supply unit
(100 - 240 V AC voltage source)
Serial interface
VGA port

Figure 7-3 mGuard centerport^2 back

7.3.1 Connecting the device

1. Optional: Install the device in a 19" frame/industrial cabinet (“Installation in a 19" frame/industrial cabinet” on page 130).
2. Connect the two mains input sockets to the mains or power supply source (100 - 240 V AC) using a mains connecting cable.
3. Connect the network connections (see “Connecting the network connections” on page 129).
4. Optional: Connect a PC monitor to the VGA port (not supplied as standard).
5. Optional: Connect a PC keyboard to one of the USB connections (not supplied as standard).

The keyboard and monitor do not need to be connected to start and operate the device. The monitor and keyboard must only be connected

- in order to use one of the boot options upon starting (booting) the device (see “Boot options - when monitor and keyboard are connected” on page 130).
- in order to perform a rescue procedure or recovery procedure. See “Restart, recovery procedure, and flashing the firmware” on page 136.

7.3.2 Connecting the network connections

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

LAN port

- Use a UTP cable (CAT5).
- Connect the LAN port of the device to the corresponding Ethernet network card of the local configuration computer or a network connection of the local network (LAN).

WAN port

- Use a UTP cable (CAT5).
- Connect the WAN port of the device to the external network or the Internet. (Connections to the remote device or network are established via this network.)

SYNC port

- Use a UTP cable (CAT5).
- Connect the SYNC port of the device to the SYNC port of a second mGuard centerport² in order to create a redundancy pair. A redundancy license for the second mGuard centerport² must be purchased separately.

DMZ port

- Use a UTP cable (CAT5).
- Connect the DMZ port of the device to a network connection of the local network (LAN). This network is used for communication according to the firewall rules of the demilitarized zone (DMZ).

IPMI port

- Use a UTP cable (CAT5).

By default, the **IPMI port** is deactivated and not documented at this point. The IPMI port functions can be activated in the BIOS setup of the motherboard. Should you have any questions on the documentation, please contact Super Micro Computer, Inc. (http://www.supermicro.com).

Serial interface

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

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

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

- A PC is connected directly to the serial interface of the mGuard (via the serial interface of the PC). The PC user can then use a terminal program to configure the mGuard via the command line.
- Or a modem is connected to the serial interface of the 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 via a modem, can then establish a PPP (Point-to Point Protocol) dial-up line connection to the mGuard and configure it via a web browser.

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

7.3.3 Installation in a 19" frame/industrial cabinet

The mains connecting cables of the power supply units are used as mains disconnect points. Sockets that can easily be accessed and that are close to the device must therefore be used for the mains plug. Unplug the mains plug to disconnect the device from the mains. If the device is installed in a control cabinet where the sockets cannot be accessed, an adequate disconnecting device must be installed during installation (e.g., an approved disconnector).

Sufficient air circulation must be ensured. If several mGuard centerport^2 devices are stacked, one or 19'' fan trays must be provided to discharge the accumulated warm air. The control cabinets used must conform to the requirements of fire-protection casings and mechanical protection according to EN 60950-1.

For information on installing the mGuard centerport^2, please refer to the “Quickrails installation instructions” provided with the device.

7.3.4 Starting (booting) the mGuard centerport^2

- Switch on the device by pressing the ON/OFF button.
- After switching on the device, the status LED lights up (green). Another LED (orange) lights up each time accessing the non-volatile memory.
- The device boots the firmware and is ready to operate.
- The display shows status messages of the mGuard firmware.

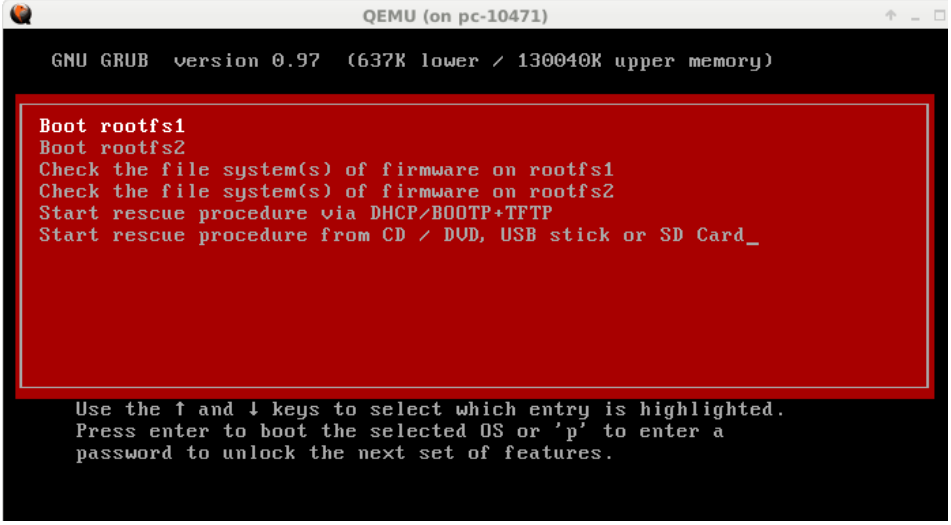
7.3.4.1 Boot options - when monitor and keyboard are connected

If a monitor and a keyboard are connected to the device, the following options are available:

- Following switch-on
- Following a restart

the boot messages from the BIOS are initially displayed on the monitor.

If the boot menu is to be displayed, press one of the direction keys several times: ↑, ↓, ← or →.



```
  GNU GRUB  version 0.97  (637K lower / 130040K upper memory)

 Boot rootfs1
 Boot rootfs2
 Check the file system(s) of firmware on rootfs1
 Check the file system(s) of firmware on rootfs2
 Start rescue procedure via DHCP/BOOTP+TFTP
 Start rescue procedure from CD / DVD, USB stick or SD Card_

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS or 'p' to enter a
    password to unlock the next set of features.
```

Figure 7-4 mGuard centerport^2 boot menu

To select and apply one of the boot options, proceed as follows:

1. Select one of the displayed options with the direction keys ↓ or ↑.
2. Then press the **Enter** button.

Boot options

Boot rootfs1

Start the primary firmware version on the device (A). This is the default setting: it is applied if the user does not intervene during startup.

Boot rootfs2

Not supported by the current firmware version.

Check the file system(s) of firmware on rootfs1

If required, checks and repairs all firmware file systems.
This menu item is only to be used in special cases when the user has the appropriate knowledge or upon instruction from the dealer support team. The mGuard firmware checks and repairs the file systems, if required, even during the normal startup process. The firmware uses its file systems in a highly robust manner when the mass storage device cache is switched off, so that there is not usually any need for repairs.

Check the file system(s) of firmware on rootfs2

Not supported by the current firmware version.

Start rescue procedure via DHCP/BootP+TFTP
Start rescue procedure from CD / DVD, USB stick or SD Card

"Restart, recovery procedure, and flashing the firmware" on page 136

7.4 Preparing the configuration

7.4.1 Connection requirements

– For the device, the two power supply units must be connected to the power supply source/to the mains. (If only one power supply unit is connected, the device can actually be operated, but it will output an acoustic signal.)

– **For local configuration**: The computer that is to be used for configuration must be connected to the LAN port on the mGuard.

– **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.

– The mGuard must be connected, i.e., the required connections must be working.

7.4.2 Local configuration on startup (router mode)

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

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

Example

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

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

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

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

7.5 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 7-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard centerport^2	Router		https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 7-3).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 136).

If the administrator web page is not displayed

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

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

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation

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

- Always click “Yes” to acknowledge the security alert.

The login window is displayed.

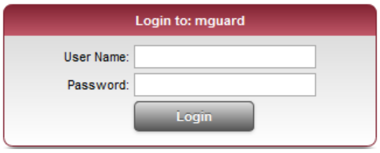


Figure 7-5 Login

- Enter your user name and password which are specified for this access type.

For access type “Administration”, the user name and password are set by default (please note these settings are case-sensitive):

UserName:	admin
Password:	mGuard

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

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

7.6 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

Configuration

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

7.7 Restart, recovery procedure, and flashing the firmware

The device must be restarted in order to perform a recovery procedure or to flash the firmware.

7.8 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the ON/OFF button of the device already started for approximately 5 s to switch off the device. (Alternatively, disconnect the power supply and then connect it again.)
- Then press the ON/OFF button again shortly to restart the device.

7.8.1 Performing a recovery procedure

Objective

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 mGuard.

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

The following network setting is restored:

Table 7-4 Restored network setting

Network mode	Management IP #1	Management IP #2
Router		https://192.168.1.1/

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

– The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.

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

– The settings configured for VPN connections and the firewall are retained, including passwords.

NOTE: After the recovery procedure has been performed successfully, a previously created configuration profile in the mGuard should be loaded and activated again. Then the network settings must be adapted.

Possible reasons for performing the recovery procedure:

– The mGuard is in PPPoE mode.

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

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

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

(Application notes are available in the download area at www.innominate.com.)

Action

Requirement: a monitor and a keyboard are connected to the device.

- Press the following keyboard shortcut: <**Alt**>**+**<**SysRq**>**+**<**a**>.

(On English keyboards the German <**S-Abf**> corresponds to <**SysRq**>. However, some keyboards do not feature the <**SysRq**> key. In this case, use the <**Print**> key.)

> After pressing the keyboard shortcut once, the same shortcut must be pressed again within 30 s in order to start the recovery procedure.

Once the recovery procedure has been performed successfully, a corresponding message appears on the monitor.

7.8.2 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

There are three options for flashing the firmware:

- Via the network (DHCP and TFTP server)
- Via the USB port (USB Flash drive or USB CD/DVD drive)
- Via the SD memory card

> The following requirements apply when loading the firmware from an **SD card**, a **USB Flash memory**:
>
> - All necessary firmware files must be located in a common directory on the first partition of the SD card or the USB Flash memory under the following path or in the following folder:
>   /Firmware/install.x86_64.p7s
>   /Firmware/firmware.img.x86_64.p7s

> The following requirements apply when loading the firmware from a **TFTP server**:
>
> - A TFTP server must be installed on the locally connected computer (see “Installing the DHCP and TFTP server” on page 258).

> - The relevant **firmware files** are available for download from the download page of www.innominate.com.

Preparation

- The mGuard firmware has been obtained from your dealer's support team or the www.innominate.com website and has been saved on the installation medium of your choice or on the local installation computer.
- If your current firmware version is newer than the version by default upon delivery, a license must be obtained for using this update. This applies to major release upgrades, e.g., from Version 6.x.y to Version 7.x.y to Version 8.x.y, etc.
- **SD card option**: The SD card has been inserted into the device.
- **USB port option**: A USB Flash memory of a USB CD/DVD driver has been connected to the USB port of the device.
- **Network option**: DHCP and TFTP servers can be accessed under the same IP address.

Action

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

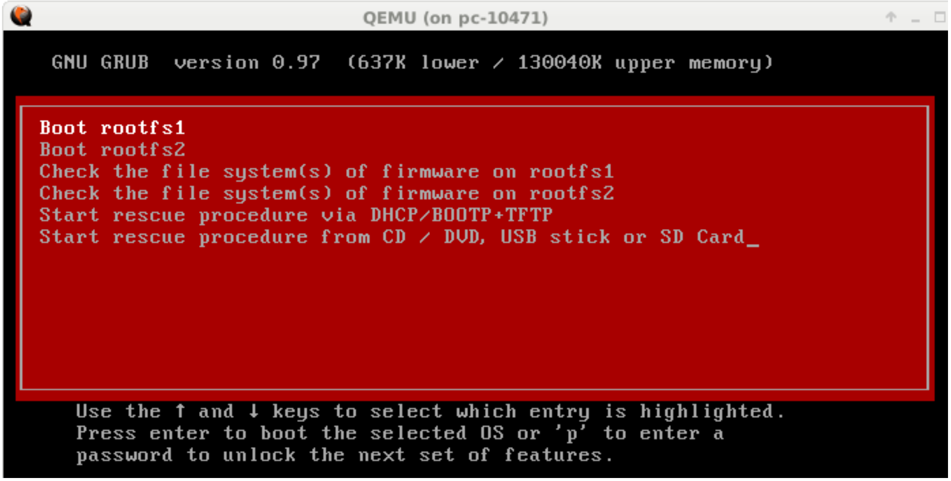
NOTE: All configured settings are deleted.

The mGuard is set to the delivery state.

In Version 5.0.0 or later of the mGuard, the licenses installed on the mGuard are retained after flashing the firmware. Therefore, they do not have to be installed again.

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

1. Restart/boot the device.
2. As soon as the device boots, press one of the arrow keys on the keyboard several times until the boot process is interrupted: ↑, ↓, ← or →.
3. The boot menu is displayed.



```
  GNU GRUB  version 0.97  (637K lower / 130040K upper memory)

 Boot rootfs1
 Boot rootfs2
 Check the file system(s) of firmware on rootfs1
 Check the file system(s) of firmware on rootfs2
 Start rescue procedure via DHCP/BOOTP+TFTP
 Start rescue procedure from CD / DVD, USB stick or SD Card_

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS or 'p' to enter a
    password to unlock the next set of features.
```

Figure 7-6 mGuard centerport² boot menu

4. Select one of the options to perform the rescue procedure using the arrow keys ↓ or ↑:

   Start rescue procedure via DHCP / BOOTP+TFTP

   OR

   Start rescue procedure from CD / DVD, USB stick or SD Card

   To apply the selection, press the **Enter** key.

   The options include:

Start rescue procedure via DHCP/BootP+TFTP

Effect: The mGuard downloads the necessary files from the TFTP server:

– install.x86_64.p7s

– firmware.img.x86_64.p7s

Start rescue procedure from CD/DVD, USB stick or SD Card

General requirements:

1. A CD/DVD drive connected to the USB port or
2. A USB stick (USB Flash drive) connected to the USB port or
3. An SD memory card inserted into the SD card drive

After the rescue procedure has been started by pressing the Enter key, the required data is downloaded from the medium that was connected/inserted to/into the device.

Start rescue procedure from CD/DVD

Requirement: The firmware of the mGuard has been previously burnt to CD/DVD (see below under “Burning the mGuard firmware to CD/DVD-ROM” on page 140).

Effect: The mGuard downloads all necessary files from the inserted CD/DVD.

With this in mind, while the boot menu is displayed and before applying this selection, insert the CD/DVD with the mGuard firmware into the CD/DVD drive.

(For security reasons, the mGuard centerport^2 does not boot from the CD/DVD).

– Once the rescue procedure is complete, a corresponding message appears on the monitor. Follow any further on-screen instructions.

Start rescue procedure from USB stick (USB Flash drive)

Requirement: The firmware of the mGuard has been previously copied to a USB storage medium (USB stick, USB Flash drive).

/Firmware/install.x86_64.p7s

/Firmware/firmware.img.x86_64.p7s

Effect: The mGuard downloads all necessary files from the connected USB storage medium. (For security reasons, the mGuard centerport^2 does not boot from the USB storage medium).

– Once the rescue procedure is complete, a corresponding message appears on the monitor. Follow any further on-screen instructions.

Start rescue procedure from SD Card

Requirement: The firmware of the mGuard has been previously copied to the SD card:
/Firmware/install.x86_64.p7s
/Firmware/firmware.img.x86_64.p7s
Effect: The mGuard downloads all necessary files from the inserted SD card. With this in mind, while the boot menu is displayed at the latest and before applying this selection, insert the SD card with the stored firmware into the mGuard. (For security reasons, the mGuard centerport^2 does not boot from an SD card).

– Once the rescue procedure is complete, a corresponding message appears on the monitor. Follow any further on-screen instructions.

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 133):

Burning the mGuard firmware to CD/DVD-ROM

The firmware for the mGuard can be burnt to CD/DVD. A zip file is available for download from the download page of www.innominate.com.

Burn the content of this zip archive as a data CD/DVD. The following files must be located in the following folders/under the following path names on the CD/DVD:

- /Firmware/install.x86_64.p7s
- /Firmware/firmware.img.x86_64.p7s

7.9 Technical data

Hardware properties	
Platform	Multi-core x86 processor architecture
Network interfaces	1 LAN port I 1 WAN port I 1 SYNC port I 1 DMZ port Ethernet IEEE 802.3 10/100/1000 Base TX I RJ45 I full/half duplex I auto MDIX
Other interfaces	VGA console I serial RS-232, D-SUB 9 connector I 6 x USB
Drives	1 HDD I 1 SD card
Redundancy options	Optional VPN license I router and firewall
Power supply	2 x 100 V AC ... 240 V AC, 300 W at 50/60 Hz, redundant
Power consumption	Dependent on the expansion stage
Humidity range	20% ... 90% during operation, non-condensing 10% ... 90% out of service
Degree of protection	Front IP20
Temperature range	0°C ... +45°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	44 mm x 447 mm x 458 mm (1 HU x 19'' x 18.5'')
Weight	9 kg

Firmware and power values	
Firmware compatibility	mGuard v8.1.2 or later; Innominate recommends using the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	2,000 Mbps bidirectional I 2,000 Mbps bidirectional When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	600 Mbps bidirectional (router mode) When using the DMZ as independent network zone, the maximum possible data throughput is distributed to the three zones.
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	Dot matrix display I LEDs I boot menu I log file I remote Syslog

Other	
Conformance	CE, developed according to UL requirements

8 mGuard delta

Table 8-1 Available mGuard delta versions

Available versions	Order No.
mGuard delta	HW-103050

As a compact LAN switch (Ethernet/Fast Ethernet), the **mGuard delta** is designed for the connection of up to four LAN segments. This device is therefore ideal for use in logically segmented network environments, where the locally connected computers/networks share the mGuard functions.

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

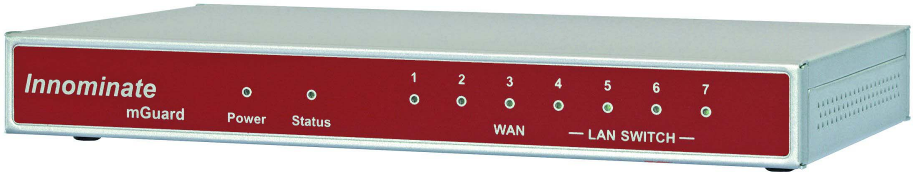


Figure 8-1 mGuard delta

8.1 Operating elements and LEDs

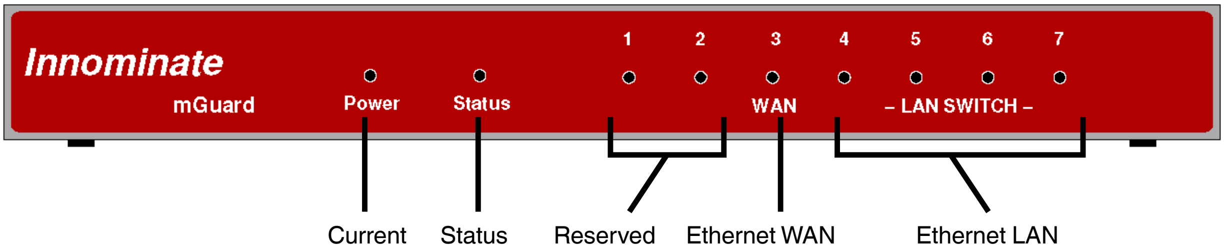


Figure 8-2 Operating elements and LEDs on the mGuard delta

Table 8-2 LEDs on the mGuard delta

LED	State	Meaning
Power	On	**The power supply is active.**
Status	On	The mGuard starts.
	Heartbeat (Flash, flash, pause, etc.)	The mGuard is ready.
1, 2	–	**Reserved**
3 (WAN)	On	**Link present**
	Flashing	Data transfer
4 - 7 (LAN)	On	Link present
	Flashing	Data transfer

8.2 Startup

8.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

– Ambient temperature:
  0°C ... +40°C
– Maximum humidity, non-condensing:
  5% ... 95%
  To avoid overheating, do not expose the mGuard to direct sunlight or other heat sources.

NOTE: Cleaning

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

8.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard delta
- Package slip
- One 5 V DC power supply
- Two UTP Ethernet cables

8.3 Connecting the 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.

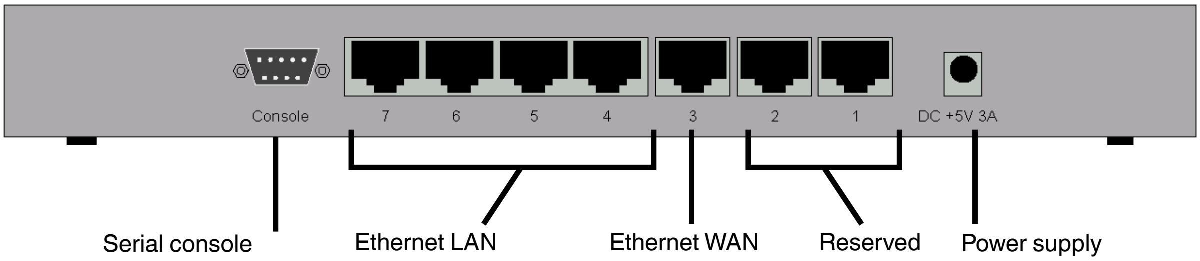


Figure 8-3 mGuard delta connections

Connecting the mGuard delta

- Connect the power supply (5 V DC, 3 A) to the “DC +5V, 3A” socket of the mGuard delta.
- Connect the local computer or the local network to one of the Ethernet LAN connections (4 to 7) of the mGuard delta using a UTP Ethernet cable (CAT5).

8.4 Preparing the configuration

8.4.1 Connection requirements

mGuard delta

- The 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 socket 4 to 7) of the mGuard,
  - Or must be connected to the mGuard via the local network.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

8.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 8-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard delta	Router	–	https://192.168.1.1/

8.4.3 Configuration in Router mode

By default upon delivery, following a reset to the default settings or after flashing the mGuard, the mGuard can be accessed within network 192.168.1.0/24 via LAN interface 4 to 7 under IP address 192.168.1.1.

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

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

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

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

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

8.5 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 8-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard delta	Router		https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 8-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 153).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 147).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

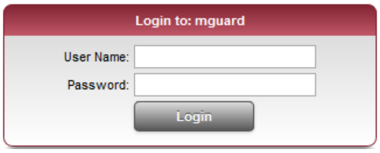


Figure 8-4 Login

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

User Name:	admin
Password:	mGuard

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

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

8.6 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer: https://123.45.67.89/

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

Configuration

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

8.7 Restart, recovery procedure, and flashing the firmware

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

– Performing a restart

– Performing a recovery procedure

– Flashing the firmware/rescue procedure

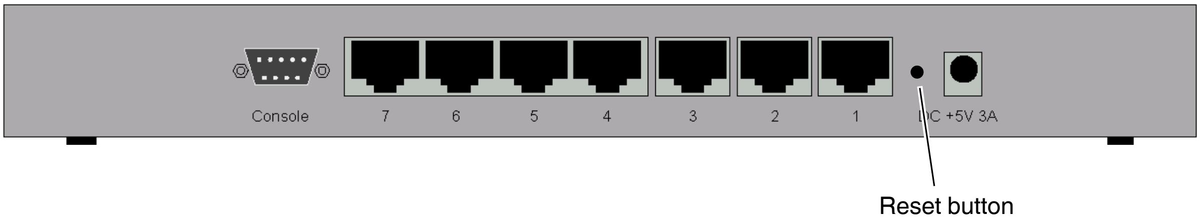


Figure 8-5 Reset button

8.7.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

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

8.7.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 8-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard delta	Router	–	https://192.168.1.1/

The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

– The mGuard is in PPPoE mode.

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

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

ℹ Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

8.7.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

NOTE: To flash the firmware, a DHCP and TFTP server or a BootP and TFTP server must be installed on the locally connected computer.

Install the DHCP and TFTP server, if necessary (see “Installing the DHCP and TFTP server” on page 258).

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

Action

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

- Hold down the Reset button until the Status LED slowly becomes dark. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The Status LED flashes.

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

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

  The Status LED flashes faster.

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

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

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.
- As soon as the procedure is complete, the Status LED flashes once a second.
- Restart the mGuard. To do this, briefly press the **Reset button**.

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

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 149):

8.8 Technical data

Hardware properties	
Platform	Intel network processor with 533 MHz clocking
Network interfaces	4 LAN ports, unmanaged switches | 1 WAN port Ethernet IEEE 802.3 10/100 Base TX | RJ45 | full duplex | auto MDIX
Other interfaces	Serial RS-232, D-SUB 9 connector
Drives	–
Redundancy options	Depending on the firmware used
Power supply	External power supply unit 5 V/3 A, DC | 110 V ... 230 V, AC
Power consumption	4.5 W, typical
Humidity range	5% ... 95% during operation, non-condensing
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	mGuard v5.0 or later: Innominate recommends firmware version 6.x or 7.x to be used with the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router | firewall)	99 Mbps bidirectional | 99 Mbps bidirectional
Hardware-based encryption	DES | 3DES | AES-128/192/256
Encrypted VPN throughput (AES-256)	70 Mbps bidirectional
Management support	Web GUI (HTTPS) | command line interface (SSH) | SNMP v1/2/3 | central device management software
Diagnostics	7 LEDs (Power, Status, WAN, LAN 1 – 4) | log file | remote syslog

Other	
Conformance	CE | FCC

9 mGuard pci

Table 9-1 Available mGuard pci versions

Available versions	Order No.
mGuard pci / 533	HW-102050
mGuard pci / 266	HW-102020
mGuard pci / 533 VPN	BD-111020
mGuard pci / 266 VPN	BD-111010

The **mGuard pci is a card which can be inserted into a PCI slot and operated in two modes.**

- In **driver mode***,* the mGuard pci provides the computer in which the card is installed with all 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.

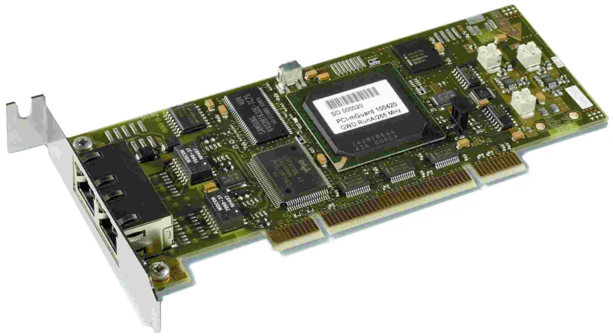


Figure 9-1 mGuard pci

9.1 Operating elements and LEDs

9.1.1 mGuard pci

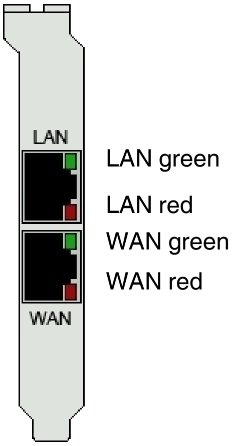


Figure 9-2 Operating elements and LEDs on the mGuard pci

Table 9-2 LEDs on the mGuard pci

LEDs	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 Reset button (for 1.5 seconds). • Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see “Performing a recovery procedure” on page 176) or contact your dealer.
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	Red/green	Various LED light codes	**Recovery mode**. After pressing the **Reset button***. See “Restart, recovery procedure, and flashing the firmware” on page 175
LAN	Green		

* On the mGuard pci, the Reset button is on the PCB (see “Installing the hardware” on page 164).

9.2 Startup

9.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

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 mGuard pci.
- Do not bend connecting cables. Only use the network plug for connection to a network.

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C ... +70°C
- Maximum humidity, non-condensing:
  20% ... 90%

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

NOTE: Cleaning

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

9.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard pci
- Package slip

9.3 Installation of mGuard pci

WARNING: This is a Class A item of equipment. This equipment can cause radio interference in residential areas; in this case, the operator may be required to implement appropriate measures.

WARNING: 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 mGuard pci.
- The mGuard is set to the desired mode using a jumper.

Driver mode

The mGuard pci can be used as a normal network card. This network card then also provides mGuard functions.

In this case, the supplied driver must be installed.

Power-over-PCI mode

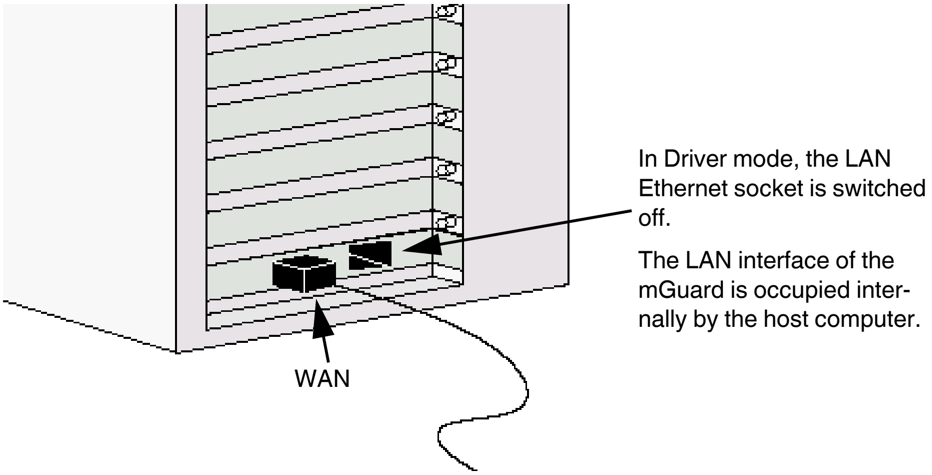
If the network card functions of the mGuard are not required or should not be used, the mGuard pci can be connected after an existing network card (on the same computer or on another) like an mGuard stand-alone device. In this operating mode, the mGuard pci actually only uses the PCI slot of a computer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

A driver is not installed.

9.3.1 Driver mode

In this mode, a driver for the PCI interface of the 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)



In Driver mode, the LAN Ethernet socket is switched off.

The LAN interface of the mGuard is occupied internally by the host computer.

Figure 9-3 Driver mode: Stealth mode

In Stealth mode, the 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 mGuard for its WAN port. This means that the 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

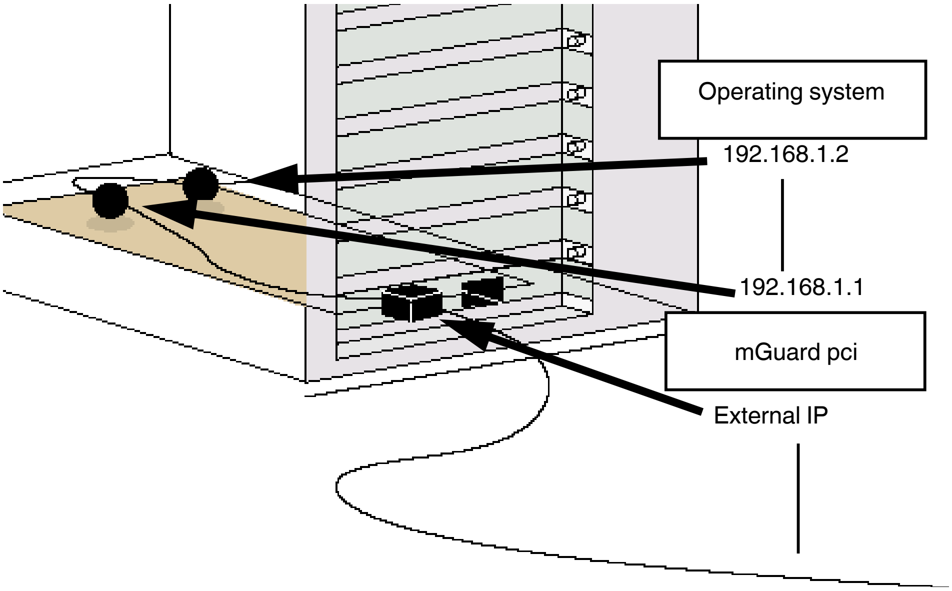


Figure 9-4 Driver mode: Router mode

If the 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 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 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 mGuard to the WAN. It is used for connection to an external network (e.g., Internet).

9.3.2 Power-over-PCI mode

Stealth mode in Power-over-PCI mode

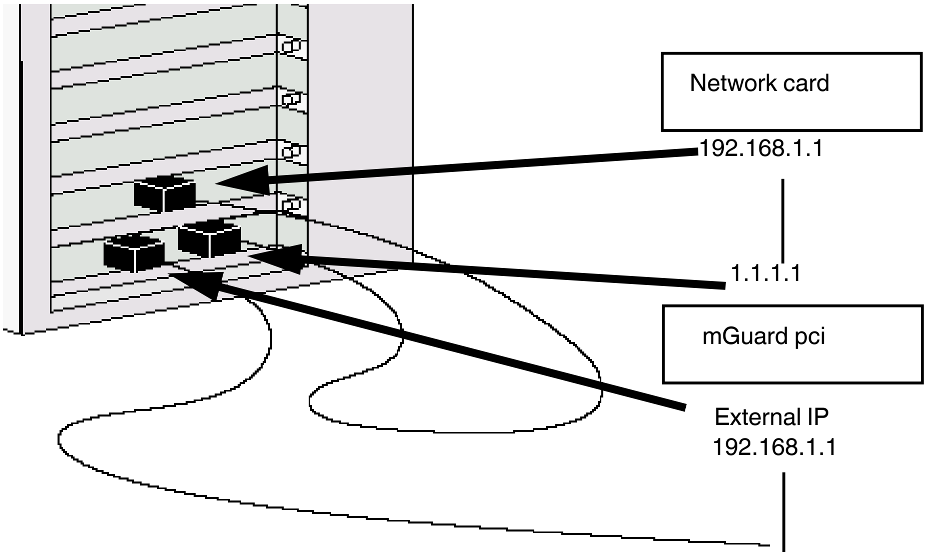


Figure 9-5 Power-over-PCI mode: Stealth mode

Since the network card functions of the 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 mGuard pci, which is located in the same computer or in another computer (see “Installing the hardware” on page 164).

In Stealth mode, the IP address configured for the network interface of the operating system (LAN port) is also used by the mGuard for its WAN port. This means that the 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

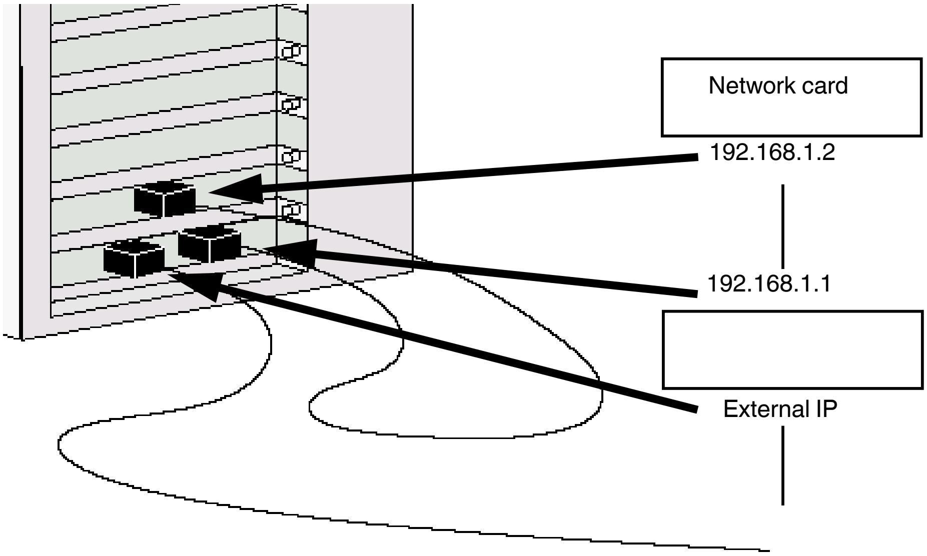


Figure 9-6 Power-over-PCI mode: Router mode

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

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

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

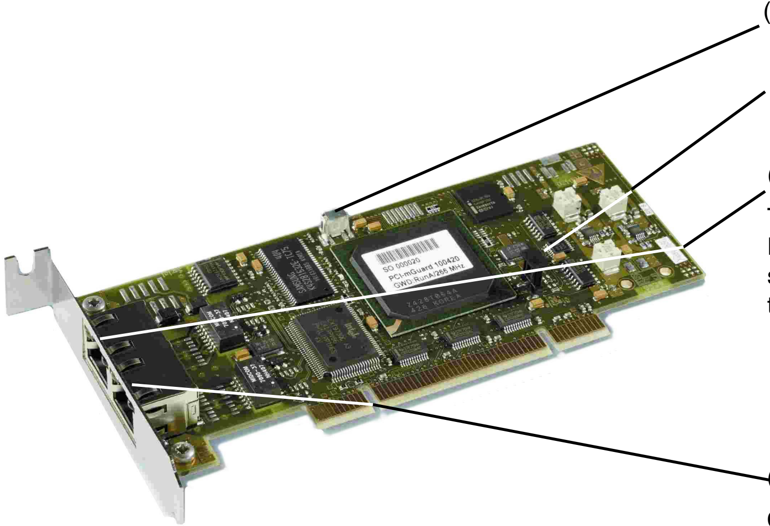
9.3.3 Installing the hardware

NOTE: Electrostatic discharge

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

The device contains components that can be damaged or destroyed by electrostatic discharge. When handling the device, observe the necessary safety precautions against electrostatic discharge (ESD) according to EN 61340-5-1 and IEC 61340-5-1.

mGuard pci: structure



(1) Reset button

(2) Jumper for activating/deactivating Driver mode

(3) LAN port

The LAN port is 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 mGuard pci for Driver mode or Power-over-PCI mode. (see “Selection of Driver mode or Power-over-PCI mode” on page 160)
- To do this, set the jumper (2) to the relevant position:

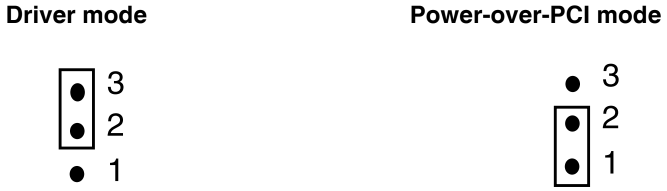


Figure 9-7 Jumper for Driver mode or Power-over-PCI mode

- 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 mGuard pci.
- Remove the corresponding slot plate by loosening the relevant screw and pulling out the slot plate.

  Keep the screw for securing the mGuard pci card.
- Carefully align the pin strip of the mGuard pci card over the socket strip of the PCI slot on the motherboard and then press the card evenly into the socket strip.
- Tighten the card slot plate.
- Close the computer cover again.
- Connect the computer power cable again and switch on the computer.

9.3.4 Installing drivers

Driver installation is only required and supported if the mGuard pci is operating in driver mode (see “Driver mode” on page 160).

Requirements

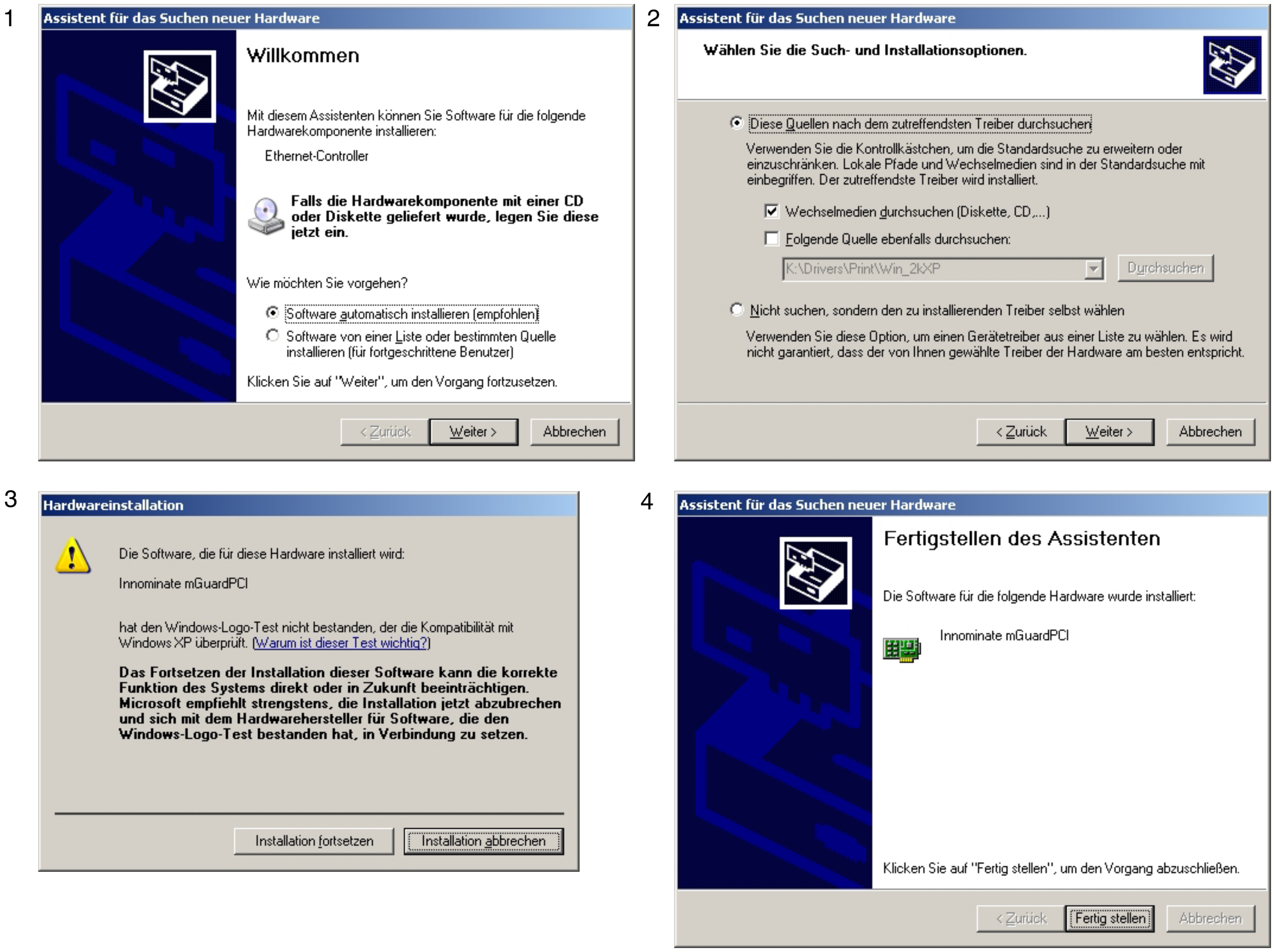
– If necessary, follow the steps described in “Installing the hardware” on page 164.
– You should have the driver files on a data carrier.

If not:

- Download the driver files from the download area at www.innominate.com.
- 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:



1

Assistent für das Suchen neuer Hardware

Willkommen

Mit diesem Assistenten können Sie Software für die folgende Hardwarekomponente installieren:

Ethernet-Controller

Falls die Hardwarekomponente mit einer CD oder Diskette geliefert wurde, legen Sie diese jetzt ein.

Wie möchten Sie vorgehen?

● Software automatisch installieren (empfohlen)

○ Software von einer Liste oder bestimmten Quelle installieren (für fortgeschrittene Benutzer)

Klicken Sie auf "Weiter", um den Vorgang fortzusetzen.

2

Assistent für das Suchen neuer Hardware

Wählen Sie die Such- und Installationsoptionen.

● Diese Quellen nach dem zutreffendsten Treiber durchsuchen

Verwenden Sie die Kontrollkästchen, um die Standardsuche zu erweitern oder einzuschränken. Lokale Pfade und Wechselmedien sind in der Standardsuche mit einbegriffen. Der zutreffendste Treiber wird installiert.

☑ Wechselmedien durchsuchen (Diskette, CD,...)

□ Folgende Quelle ebenfalls durchsuchen:

K:\Drivers\Print\Win_2kXP

○ Nicht suchen, sondern den zu installierenden Treiber selbst wählen

Verwenden Sie diese Option, um einen Gerätetreiber aus einer Liste zu wählen. Es wird nicht garantiert, dass der von Ihnen gewählte Treiber der Hardware am besten entspricht.

3

Hardwareinstallation

Die Software, die für diese Hardware installiert wird:

Innominate mGuardPCI

hat den Windows-Logo-Test nicht bestanden, der die Kompatibilität mit Windows XP überprüft. (Warum ist dieser Test wichtig?)

Das Fortsetzen der Installation dieser Software kann die korrekte Funktion des Systems direkt oder in Zukunft beeinträchtigen. Microsoft empfiehlt strengstens, die Installation jetzt abzubrechen und sich mit dem Hardwarehersteller für Software, die den Windows-Logo-Test bestanden hat, in Verbindung zu setzen.

4

Assistent für das Suchen neuer Hardware

Fertigstellen des Assistenten

Die Software für die folgende Hardware wurde installiert:

Innominate mGuardPCI

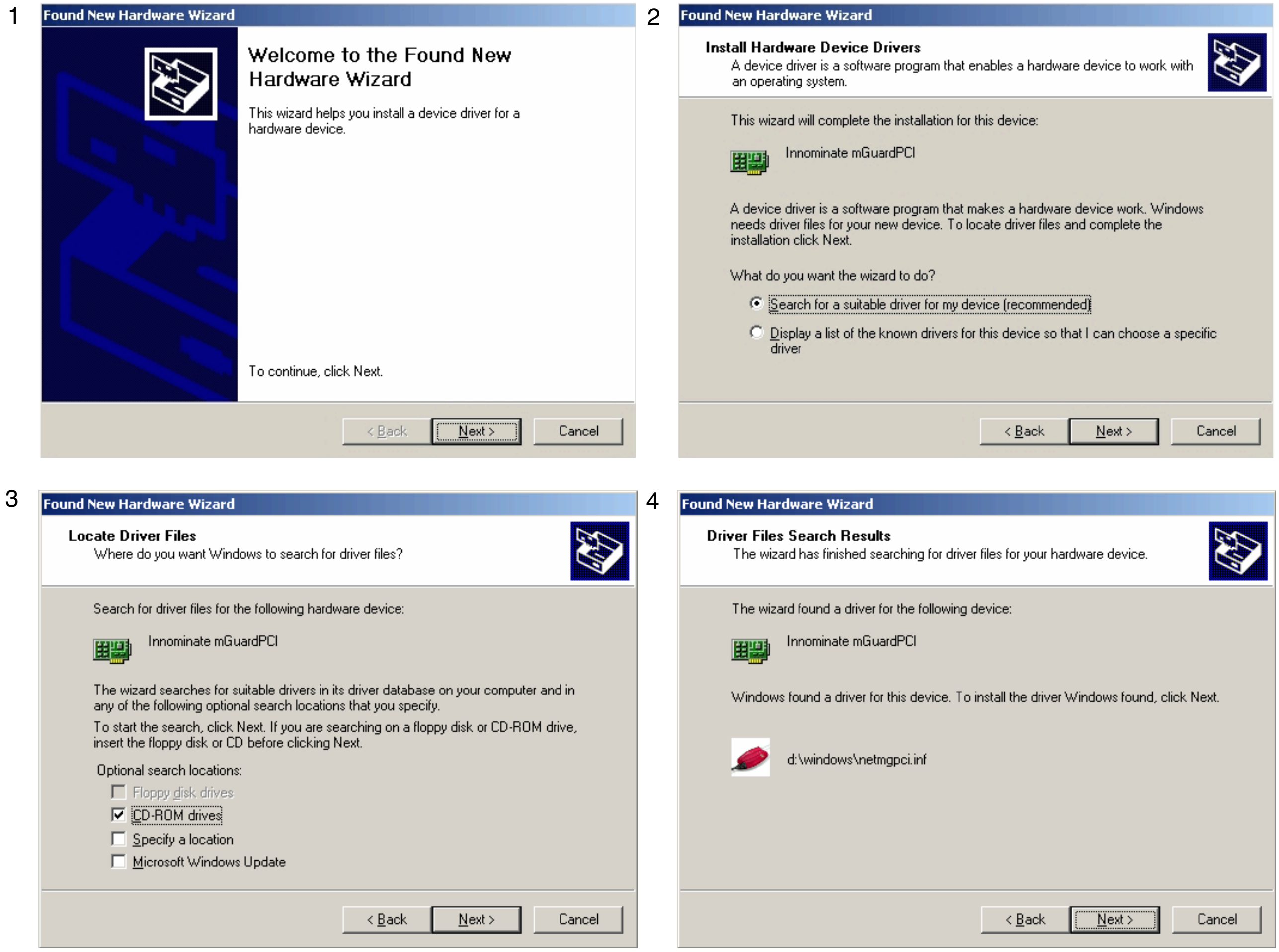
Klicken Sie auf "Fertig stellen", um den Vorgang abzuschließen.

Figure 9-8 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 “Continue Anyway”.
4. Click “Finish”

Under Windows 2000

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



1 Found New Hardware Wizard

Welcome to the Found New Hardware Wizard

This wizard helps you install a device driver for a hardware device.

To continue, click Next.

2 Found New Hardware Wizard

Install Hardware Device Drivers

A device driver is a software program that enables a hardware device to work with an operating system.

This wizard will complete the installation for this device:

Innominate mGuardPCI

A device driver is a software program that makes a hardware device work. Windows needs driver files for your new device. To locate driver files and complete the installation click Next.

What do you want the wizard to do?

● Search for a suitable driver for my device (recommended)

○ Display a list of the known drivers for this device so that I can choose a specific driver

3 Found New Hardware Wizard

Locate Driver Files

Where do you want Windows to search for driver files?

Search for driver files for the following hardware device:

Innominate mGuardPCI

The wizard searches for suitable drivers in its driver database on your computer and in any of the following optional search locations that you specify.

To start the search, click Next. If you are searching on a floppy disk or CD-ROM drive, insert the floppy disk or CD before clicking Next.

Optional search locations:

☐ Floppy disk drives
☑ CD-ROM drives
☐ Specify a location
☐ Microsoft Windows Update

4 Found New Hardware Wizard

Driver Files Search Results

The wizard has finished searching for driver files for your hardware device.

The wizard found a driver for the following device:

Innominate mGuardPCI

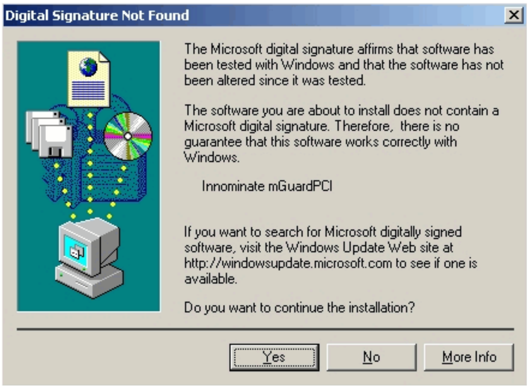
Windows found a driver for this device. To install the driver Windows found, click Next.

d:\windows\netmgpci.inf

Figure 9-9 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”.

5



Digital Signature Not Found

The Microsoft digital signature affirms that software has been tested with Windows and that the software has not been altered since it was tested.

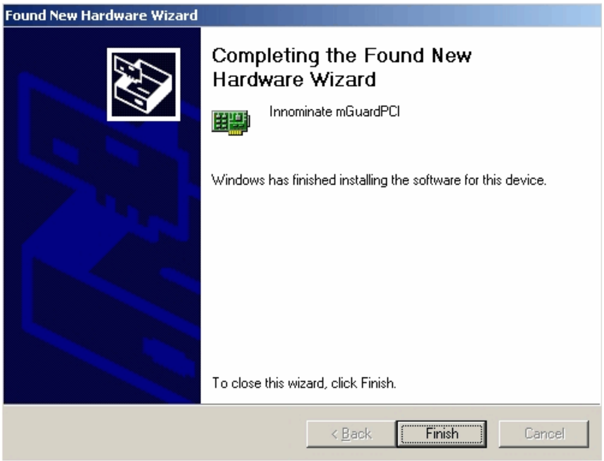
The software you are about to install does not contain a Microsoft digital signature. Therefore, there is no guarantee that this software works correctly with Windows.

Innominate mGuardPCI

If you want to search for Microsoft digitally signed software, visit the Windows Update Web site at http://windowsupdate.microsoft.com to see if one is available.

Do you want to continue the installation?

6



Found New Hardware Wizard

Completing the Found New Hardware Wizard

Innominate mGuardPCI

Windows has finished installing the software for this device.

To close this wizard, click Finish.

Figure 9-10 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
```

9.4 Preparing the configuration

9.4.1 Connection requirements

mGuard pci

- **For local configuration**: The computer used for configuration must meet the following requirements:
  - mGuard **in Driver mode**: The mGuard pci driver must be installed on the computer.
  - mGuard in Power-over-PCI mode: The computer must be connected to the LAN connection of the mGuard or to the mGuard via the local network.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

9.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 9-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard pci	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see page 172). Alternatively, you can select a different stealth configuration or use another network mode.

9.5 Configuration in Stealth mode

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 164.

Installing the drivers

- If you have configured the mGuard for **Driver mode**, make sure that the drivers are installed as described under “Installing drivers” on page 165.

Configuring the network interface

If the mGuard

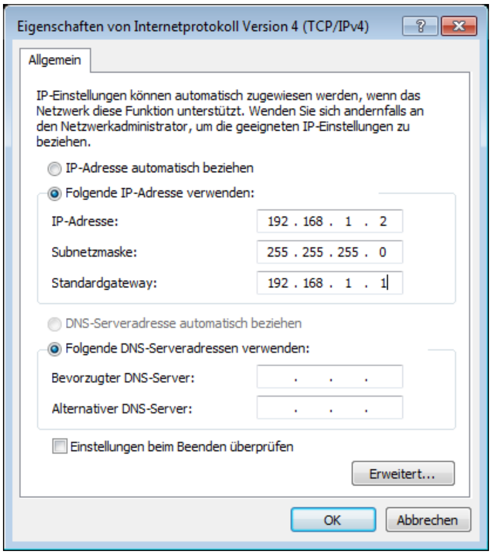
– Is operated in **Driver mode** and the LAN interface (network interface of the computer) has not yet been configured or

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

This network interface must be configured before the 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:



Eigenschaften von Internetprotokoll Version 4 (TCP/IPv4)

Allgemein

IP-Einstellungen können automatisch zugewiesen werden, wenn das Netzwerk diese Funktion unterstützt. Wenden Sie sich andernfalls an den Netzwerkadministrator, um die geeigneten IP-Einstellungen zu beziehen.

○ IP-Adresse automatisch beziehen

● Folgende IP-Adresse verwenden:

IP-Adresse: 192 . 168 . 1 . 2

Subnetzmaske: 255 . 255 . 255 . 0

Standardgateway: 192 . 168 . 1 . 1

○ DNS-Serveradresse automatisch beziehen

● Folgende DNS-Serveradressen verwenden:

Bevorzugter DNS-Server: . . .

Alternativer DNS-Server: . . .

□ Einstellungen beim Beenden überprüfen

Figure 9-11 Internet Protocol (TCP/IP) Properties

Default gateway

Once you have configured the network interface, you should be able to access the mGuard's configuration interface with a web browser by going to 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 170 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
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

  Do not under any circumstances assign an address such as 1.1.1.2 to the configuration computer.

- 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 172).
- 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 mGuard, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

9.6 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 9-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard pci	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 9-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 176).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 169).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

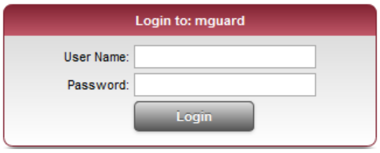
Once a connection has been established successfully, a security alert may be displayed.

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.



Login to: mguard

User Name:

Password:

Figure 9-12 Login

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

User Name:	admin
Password:	mGuard

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

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

9.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

Configuration

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

9.8 Restart, recovery procedure, and flashing the firmware

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

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

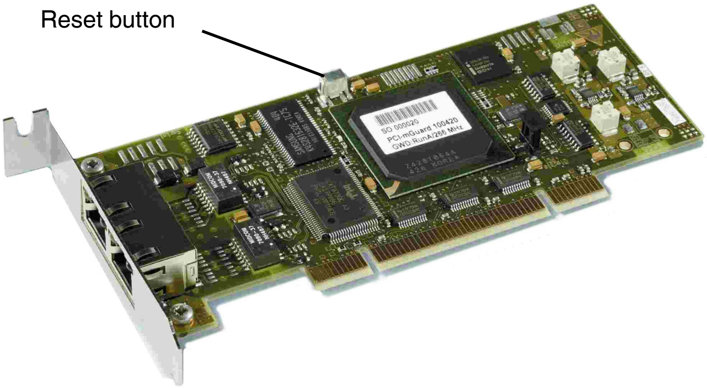


Figure 9-13 Reset button

9.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until both red LEDs light up.
  Alternatively, restart the computer that contains the mGuard pci card.

9.8.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 9-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard pci	Stealth	https://1.1.1.1/	https://192.168.1.1/

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

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

Possible reasons for performing the recovery procedure:

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

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

9.8.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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 258).

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

- If the mGuard is operated in **Power-over-PCI mode**, the DHCP/TFTP server must be connected via the LAN socket of the mGuard.
- If the mGuard is operated in PCI **Driver mode**, the DHCP/TFTP server must be operated on the computer or operating system that the interface provides for the mGuard.

Action

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

- Hold down the Reset button until the green LEDs and the red LAN LED light up. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The red LAN LED flashes.

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

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

  The green LEDs and the red LAN LED form a running light.

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

  This process takes around 3 to 5 minutes. The green LEDs flash, while the red LAN LED is lit continuously.

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.
- As soon as the procedure has been completed, the mGuard restarts.

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 172):

After the restart, the **mGuard pci** is automatically assigned a management IP address. This address is assigned by a BootP server that can be accessed on the network and was used during flashing.

If the recommended DHCP server is also used for Windows (see page 258), it also operates as the BootP server. This does not apply when using a DHCP server under Linux.

9.9 Technical data

mGuard pci /266 | mGuard pci /533

Hardware properties	
Platform	Intel network processor Optionally with 266 MHz or 533 MHz clocking
Network interfaces	1 LAN port | 1 WAN port Ethernet IEEE 802.3 10/100 Base TX | RJ45 | full duplex | auto MDIX
Other interfaces	Serial RS-232, internal connector
Drives	–
Redundancy options	Depending on the firmware used
Power supply	3.3 V or 5 V, via PCI bus
Power consumption	Typical, 3.7 W ... 4.2 W
Humidity range	20% ... 90% during operation, non-condensing
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	mGuard v5.0 or later: Innominate recommends firmware version 6.x or 7.x to be used with the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router | firewall)	99 Mbps bidirectional | 99 Mbps bidirectional
Hardware-based encryption	DES | 3DES | AES-128/192/256
Encrypted VPN throughput (AES-256)	35 Mbps (PCI /256) bidirectional | 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, system error, Ethernet status, Recovery mode) | Log File | Remote Syslog

Other	
Conformance	CE | FCC | UL 508 | Operating modes with/without driver via PoPCI

10 mGuard blade

Table 10-1 Available versions

Available versions	Order No.
mGuard blade / 533	HW-104050
mGuard blade / 266	HW-104020
mGuard bladebase	HW-104500
mGuard bladepack / 533	HW-104850
mGuard bladepack / 266	HW-104820

The **mGuard blade** consists of the mGuard bladebase, which can be built into standard 3-U racks (19 inch) without problems and accommodate up to 12 mGuard blades and one 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 connection or a terminal.

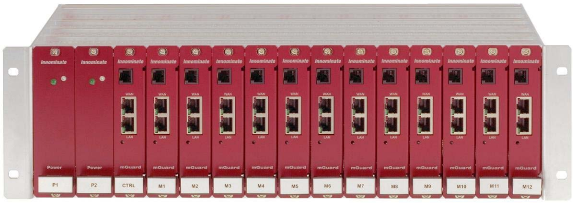


Figure 10-1 mGuard blade

10.1 Operating elements and LEDs

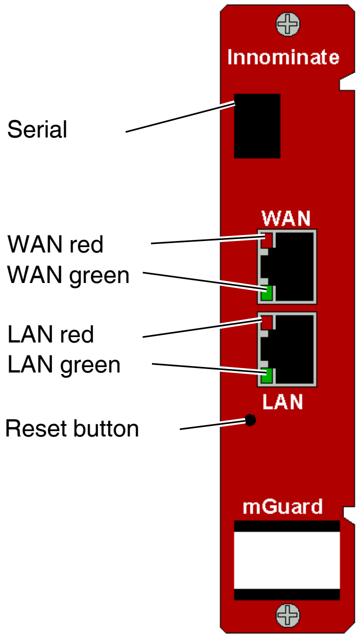


Figure 10-2 Operating elements and LEDs on the mGuard blade

Table 10-2 mGuard blade

LED	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 Reset button (for 1.5 seconds). If the error is still present, start the recovery procedure (see “Performing a recovery procedure” on page 193) or contact your dealer.
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	Red/green	Various LED light codes	**Recovery mode**. After pressing the **Reset button**. See “Restart, recovery procedure, and flashing the firmware” on page 192
LAN	Green		

10.2 Startup

10.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:
  +5°C ... +40°C
- Maximum humidity, non-condensing:
  10% ... 95%

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

NOTE: Cleaning

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

10.2.2 Checking the scope of supply

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

The scope of supply includes:

- Package slip
- 19" mGuard bladebase
- An 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 mGuard bladebase

10.3 Installation of mGuard blade

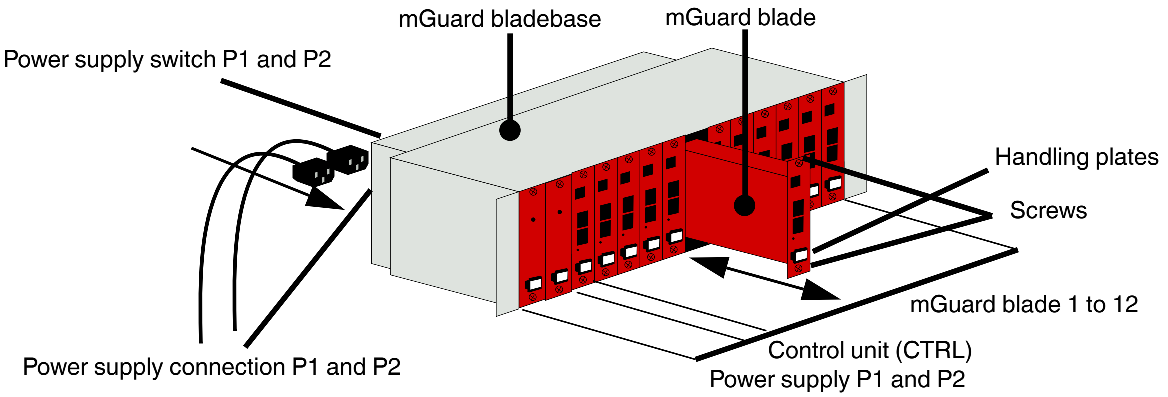


Figure 10-3 Installation of mGuard blade

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.

Installation of mGuard bladebase

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

Installation of mGuard blade

The mGuard bladebase does not have to be switched off when installing or removing an mGuard blade.

- Loosen the top and bottom screw on the faceplate or on the mGuard blade to be replaced.
- Remove the faceplate or pull out the old mGuard blade.
- Insert the new mGuard blade and PCB into the plastic guides and push it completely into the mGuard bladebase.
- Secure the mGuard blade by tightening the screws slightly.
- Replace the empty handling plate with the suitable number from the mGuard bladebase accessories or replace it with the plate from the old 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 supplies. An mGuard blade operated in this slot acts as the controller (control unit) for all other mGuard blade devices.

During initial installation of an 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 mGuard blade

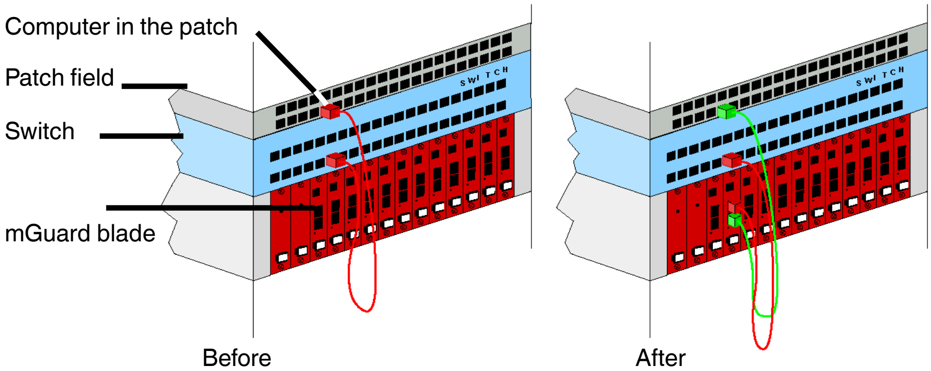


Figure 10-4 Connecting the mGuard blade to the network

NOTE: If your computer is already connected to a network, patch the 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 mGuard blocks 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 socket) must not be connected directly to telecommunications connections. To connect a serial terminal or a modem, use a serial cable with RJ12 plug. The maximum cable length of the serial cable is 30 m.

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

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

- A PC is connected directly to the serial interface of the mGuard (via the serial interface of the PC). The PC user can then use a terminal program to configure the mGuard via the command line.
- Alternatively, a modem may be connected to the serial interface of the 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 connection to the mGuard and configure it via a web browser.

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

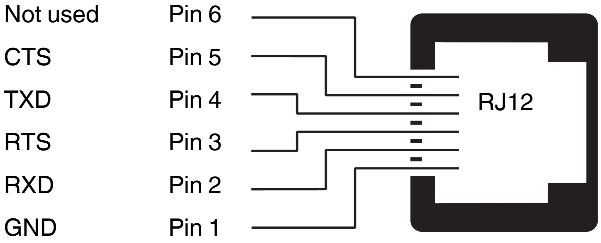


Figure 10-5 Pin assignment of the RJ12 socket (serial port)

10.4 Preparing the configuration

10.4.1 Connection requirements

- The mGuard blade must be mounted in the 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 socket of the mGuard
  - Or the computer must be connected to the mGuard via the network.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

10.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 10-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard blade controller	Router	–	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (see Page 189). Alternatively, you can select a different stealth configuration or use another network mode.

10.4.3 Configuring the mGuard with the Router mode default setting

By default upon delivery, following a reset to the default setting or after flashing the mGuard, the device can be accessed within network 192.168.1.0/24 via the LAN interface (for mGuard blade LAN interfaces 4 to 7) under IP address 192.168.1.1.

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

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

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

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

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

10.5 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 10-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard blade controller	Router	–	https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 10-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 193).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 187).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

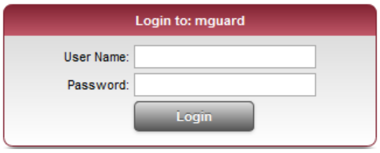


Figure 10-6 Login

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

User Name:	admin
Password:	mGuard

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

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

10.6 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

Configuration

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

10.7 Restart, recovery procedure, and flashing the firmware

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

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

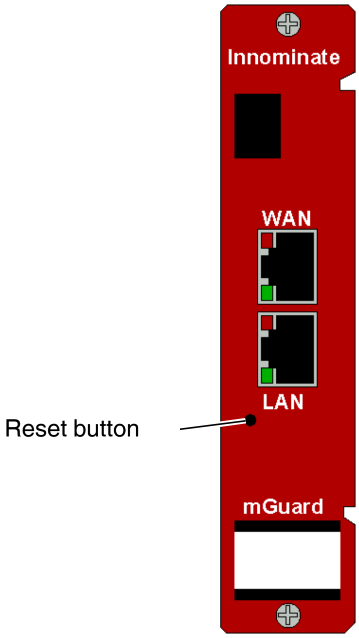


Figure 10-7 Reset button

10.7.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until both red LEDs light up. (Alternatively, disconnect the power supply and then connect it again.)

10.7.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 10-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard blade controller	Router	–	https://192.168.1.1/

The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

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

ℹ Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: www.innominate.com.

Action

- Slowly press the Reset button six times.

  After approximately 2 seconds, the LAN LED lights up red.
- Press the Reset button slowly again six times.

  If successful, the LAN LED lights up red.
  If unsuccessful, the WAN LED lights up red.

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

10.7.3 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

Requirements for flashing

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 258).

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

Action

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

- Hold down the Reset button until the green LEDs and the red LAN LED light up. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The red LAN LED flashes.

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

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

  The green LEDs and the red LAN LED form a running light.

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

  This process takes around 3 to 5 minutes. The green LEDs flash, while the red LAN LED is lit continuously.

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.
- As soon as the procedure has been completed, the mGuard restarts.

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 189).

10.8 Technical data

mGuard blade /266 | mGuard blade /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 | RJ45 | full duplex | auto MDIX
Other interfaces	Serial RS-232, RJ11 socket
Drives	–
Redundancy options	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, non-condensing
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 | *bladepack*: 7.7 kg

Firmware and power values	
Firmware compatibility	mGuard v5.0 or later: Innominate recommends firmware version 6.x or 7.x to be used with the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router | firewall)	99 Mbps bidirectional | 99 Mbps bidirectional
Hardware-based encryption	DES | 3DES | AES-128/192/256
Encrypted VPN throughput (AES-256)	35 Mbps (blade /256) bidirectional | 70 Mbps (blade /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, system error, Ethernet status, Recovery mode) | Log File | Remote Syslog

Other	
Conformance	CE | FCC

11 mGuard centerport

Table 11-1 Available mGuard centerport versionsf

Available versions	Order No.
mGuard centerport	HW-106000
mGuard centerport VPN-250	BD-601000
mGuard centerport VPN-1000	BD-602000

The **mGuard centerport** is a high-end firewall and a VPN gateway in 19" format. It is suitable as a central network infrastructure for remote service solutions, With its Gigabit Ethernet interfaces and corresponding throughput as the router and as the stateful inspection firewall, the device can also be used in the backbone in industrial networks.

As a gateway, the mGuard centerport supports the VPN connection to any number of systems in the VPN tunnel groups with up to a thousand simultaneous tunnels, which all belong to the same unique public IP address.

The mGuard centerport performs secure remote services, such as remote support, remote diagnostics, remote maintenance, and condition monitoring for a large number of machines and systems via the Internet. An encrypted VPN data throughput of 600 Mbps is possible to one interface.

The mGuard centerport is compatible with all mGuard VPN field devices and the mGuard device manager.

The mGuard centerport can be provided in three device versions, which determine the number of simultaneously supported active VPN tunnels: mGuard centerport, mGuard centerport 250, mGuard centerport 1000.

Figure 11-1 mGuard centerport

11.1 Operating elements and LEDs

Front

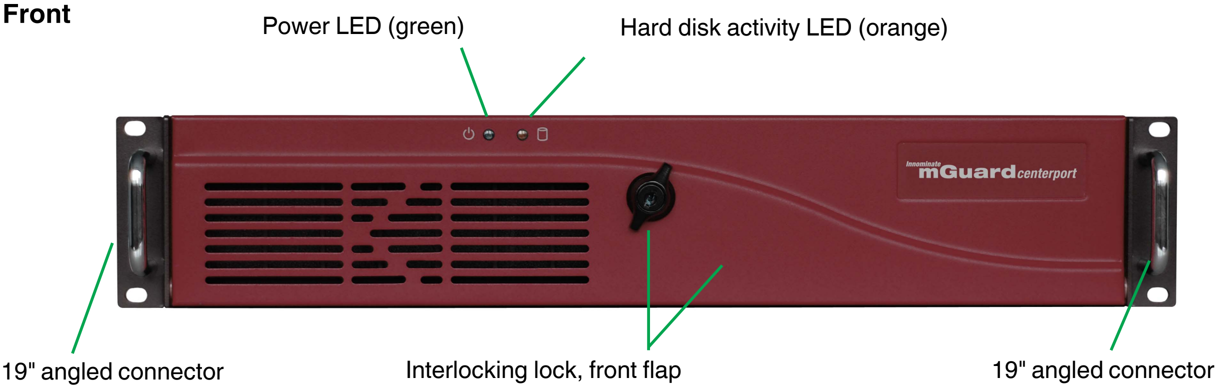

Power LED (green)
Hard disk activity LED (orange)
19" angled connector
Interlocking lock, front flap
19" angled connector

Figure 11-2 Operating elements and LEDs on the mGuard centerport front side

Table 11-2 LEDs on the mGuard centerport

LED	State	Meaning
Green	On	Lights up if the system is switched on
Orange	On	Lights up while hard disk is accessed

Front flap open

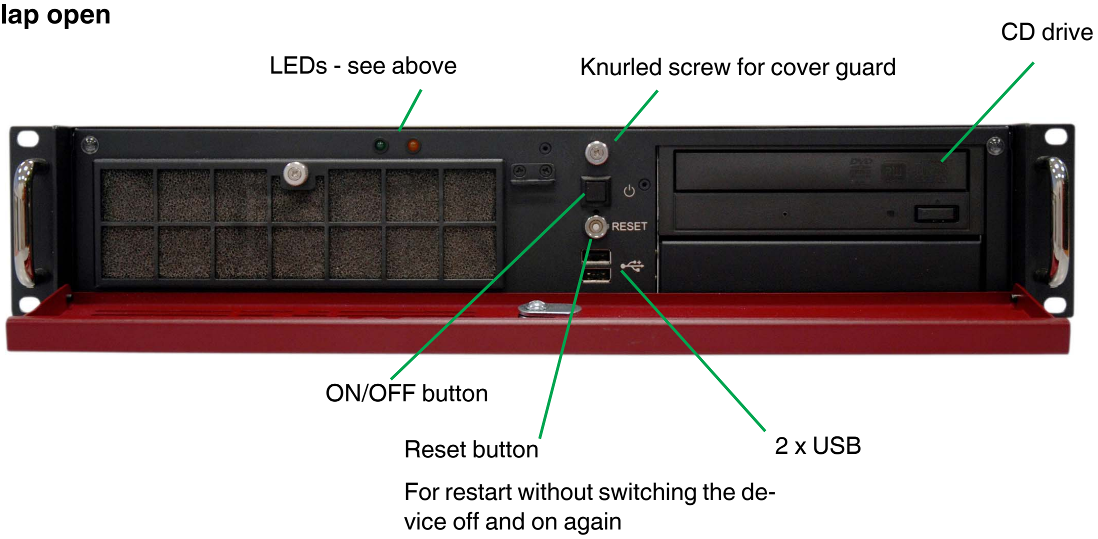

CD drive
LEDs - see above
Knurled screw for cover guard
ON/OFF button
Reset button
For restart without switching the device off and on again
2 x USB

Figure 11-3 Operating elements for the mGuard centerport with front flap open

11.2 Startup

11.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C ... +40°C
- Maximum humidity, non-condensing:
  5% ... 95%

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

NOTE: Cleaning

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

11.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard centerport
- Package slip
- 2 x keys for front flap lock
- 2 x AC mains connecting cables
- Rubber feet (self-adhesive)

11.3 Installing and booting mGuard centerport

Back

Unnamed connections/sockets are not used.

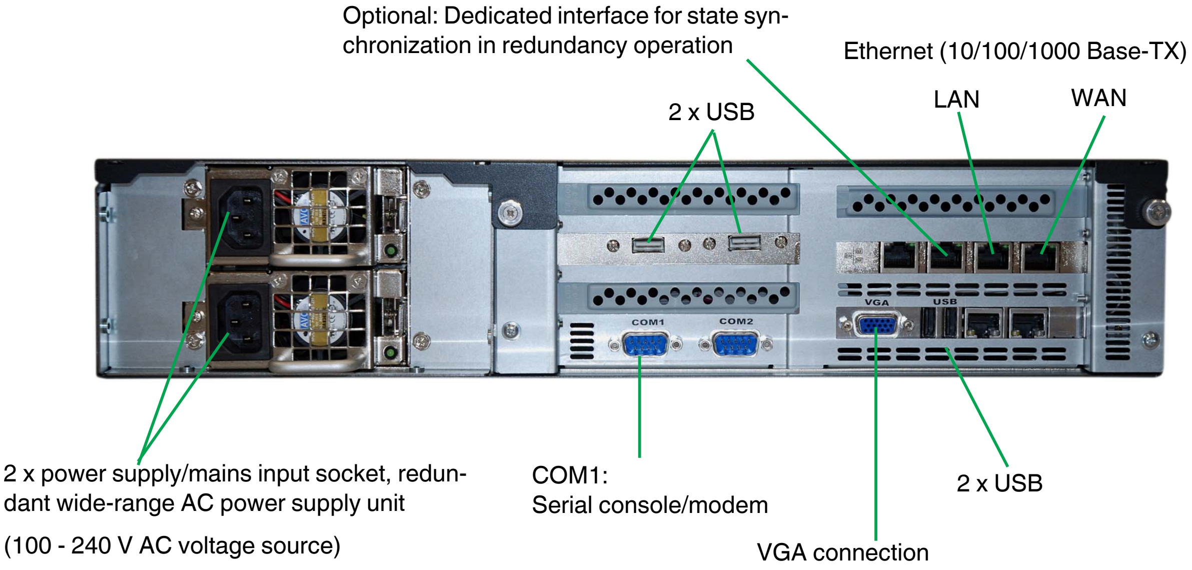

Optional: Dedicated interface for state synchronization in redundancy operation
Ethernet (10/100/1000 Base-TX)
LAN
WAN
2 x USB
COM1
COM2
VGA
USB
2 x power supply/mains input socket, redundant wide-range AC power supply unit
(100 - 240 V AC voltage source)
COM1:
Serial console/modem
2 x USB
VGA connection

Figure 11-4 mGuard centerport back

11.3.1 Connecting the device

7. Optional:

   Install the device in a 19" industrial cabinet - see “The safety lock on the front flap enables the front flap to be securely locked, so that access is refused to the drives, reset button, and ON/OFF switch. Ensure that you keep safe hold of the two keys provided-Housing” on page 202.
8. Connect the two power supply units to the mains or power supply source via the two mains input sockets (100 - 240 V AC).
9. Connect the network connections - see “Connecting network connections” on page 201.
10. Optional:

    Connect a PC monitor to the **VGA port** (not supplied as standard).

    Connect a PC keyboard to one of the **USB** connections (not supplied as standard).

    The monitor and keyboard must only be connected

    – in order to use one of the boot options upon starting (booting) mGuard centerport - see “Boot options - when monitor and keyboard are connected” on page 202,

    – in order to perform a rescue procedure or recovery procedure. See “Restart, recovery procedure, and flashing the firmware” on page 209

    The keyboard and monitor do not need to be connected to start and operate the device.

11.3.2 Connecting network connections

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

LAN port

- Connect the local computer or the local network to the LAN port of the mGuard using a UTP Ethernet cable (CAT5).

WAN port

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

COM1: Serial port

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

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

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

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

– Or a modem is connected to the serial interface of the 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 connection to the mGuard and configure it via a web browser.

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

11.3.3 Front flap

The safety lock on the front flap enables the front flap to be securely locked, so that access is refused to the drives, reset button, and ON/OFF switch. Ensure that you keep safe hold of the two keys providedHousing

The mGuard centerport housing is from Kontron and is referred to as the KISS 2U platform. Visit www.kontron.de for more information on the following:

- Mounting in a 19" industrial cabinet
- Mounting of housing feet
- Removing the 19" angled connector from the device
- Maintenance and care

11.3.4 Starting (booting) mGuard centerport

- Press the ON/OFF button

The mGuard centerport boots the firmware and is ready to operate.

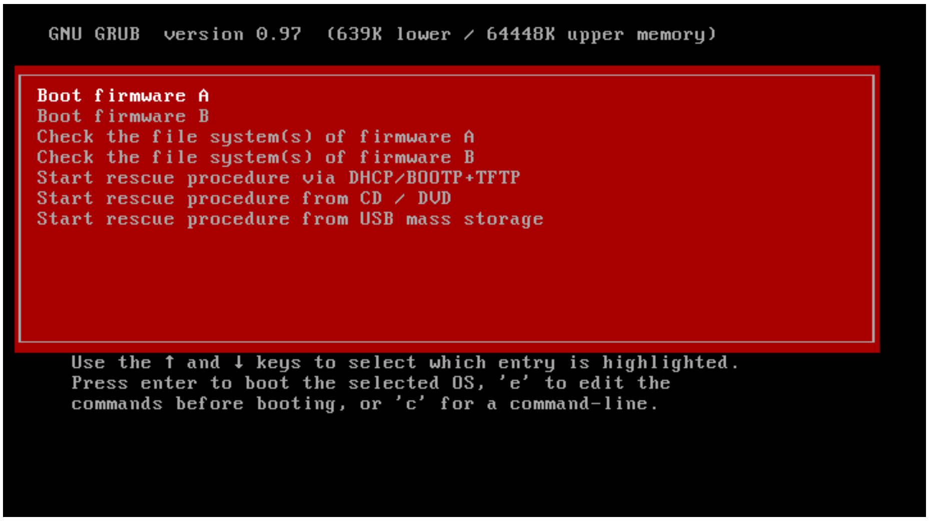
11.3.4.1 Boot options - when monitor and keyboard are connected

If a monitor and a keyboard are connected to the device, the following options are available:

- Following switch-on
- Following a restart
- After pressing the Reset button

If the boot messages from the BIOS are initially displayed on the monitor, the mGuard centerport boot menu is shown for a few seconds.

If the boot menu is displayed for a longer period of time, preferably press one of the following direction keys: ↑, ↓, ← or →.



```
 GNU GRUB  version 0.97  (639K lower / 64448K upper memory)

 Boot firmware A
 Boot firmware B
 Check the file system(s) of firmware A
 Check the file system(s) of firmware B
 Start rescue procedure via DHCP/BOOTP+TFTP
 Start rescue procedure from CD / DVD
 Start rescue procedure from USB mass storage

    Use the ↑ and ↓ keys to select which entry is highlighted.
    Press enter to boot the selected OS, 'e' to edit the
    commands before booting, or 'c' for a command-line.
```

Figure 11-5 mGuard centerport boot menu

To select and apply one of the boot options, proceed as follows:

1. Select one of the displayed options with the direction keys ↓ or ↑.
2. Then press the **Enter** button.

Boot options

Boot firmware A

Start the primary firmware version on the device (A). The default setting: it is applied if the user does not intervene during startup.

Boot firmware B

Not supported by the current firmware version.

Check the file system(s) of firmware A

If required, checks and repairs all firmware file systems.

This menu item is only to be used in special cases when the user has the appropriate knowledge or upon instruction from the dealer support team. The mGuard firmware checks and repairs the file systems, if required, even during the normal startup process. The firmware uses its file systems in a highly robust manner when the mass storage device cache is switched off, so that there is not usually any need for repairs.

Check the file system(s) of firmware B

Not supported by the current firmware version.

Start rescue procedure via DHCP/BootP+TFTP
Start rescue procedure from CD/DVD
Start rescue procedure from USB mass storage

"Restart, recovery procedure, and flashing the firmware" on page 209

11.4 Preparing the configuration

11.4.1 Connection requirements

- For mGuard centerport, the two power supply units must be connected to the power supply source/to the mains. (If only one power supply unit is connected, the device can actually be operated, but it will output an acoustic signal.)
- **For local configuration**: The computer that is to be used for configuration must be connected to the LAN socket on the mGuard.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

11.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 11-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard centerport	Router		https://192.168.1.1/

11.4.3 Configuration in Router mode

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

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

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

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

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

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

11.5 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 11-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard centerport	Router		https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 11-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 210).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 204).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

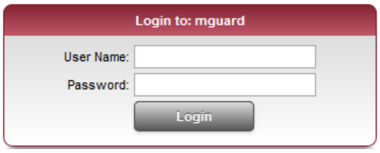


Figure 11-6 Login

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

User Name:	admin
Password:	mGuard

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

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

11.6 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer: https://123.45.67.89/

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

Configuration

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

11.7 Restart, recovery procedure, and flashing the firmware

For mGuard centerport, there is a reset key which can be used to perform a restart. The rescue procedure and therefore the reloading of mGuard firmware is initiated via the boot menu.

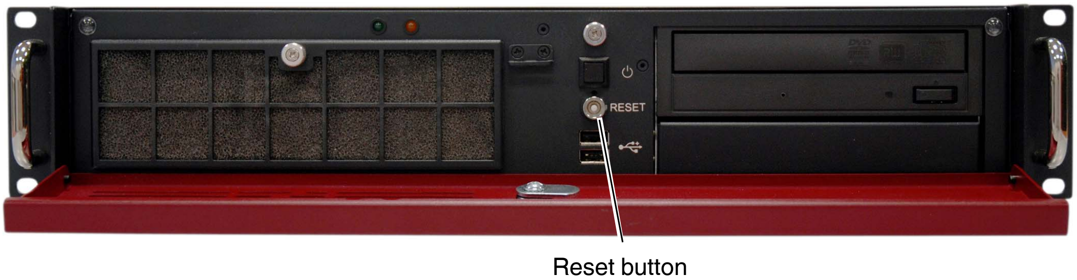


Figure 11-7 Reset button

11.8 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button.
  (Alternatively, disconnect the power supply and then connect it again.)

11.8.1 Performing a recovery procedure

Objective

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 mGuard.

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

Table 11-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard centerport	Router		https://192.168.1.1/

The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

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

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

(Application notes are available in the download area at www.innominate.com.)

Action

Requirement: a monitor and a keyboard are connected to the device.

- Press the following keyboard shortcut: <**Alt**>**+**<**SysRq**>**+**<**a**>.

(On English keyboards the German <S-Abf> corresponds to <SysRq>. However, some keyboards do not feature the <SysRq> key. In this case, use the <Print> key.)

Once the recovery procedure is complete, a corresponding message appears on the monitor.

11.8.2 Flashing the firmware/rescue procedure

Objective

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

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

Possible reasons

The administrator and root password have been lost.

Requirements

NOTE: To flash the firmware, a DHCP and TFTP server or a BootP and TFTP server must be installed on the locally connected computer.

Install the DHCP and TFTP server, if necessary (see “Installing the DHCP and TFTP server” on page 258).

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

- A monitor and a keyboard are connected to the device.
- The mGuard firmware has been obtained from the Support team of your dealer or from www.innominate.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.

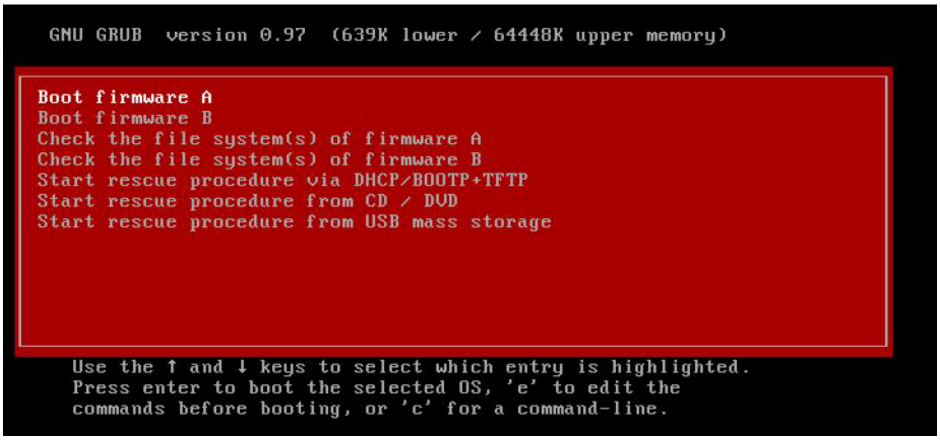
Action

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

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

1. Restarting/booting the mGuard centerport.
2. As soon as the mGuard centerport boot menu appears on the monitor, preferably press one of the following direction keys: ↑, ↓, ← or →.

   The boot menu then continues to be displayed.



```
  GNU GRUB  version 0.97  (639K lower / 64448K upper memory)

   Boot firmware A
   Boot firmware B
   Check the file system(s) of firmware A
   Check the file system(s) of firmware B
   Start rescue procedure via DHCP/BOOTP+TFTP
   Start rescue procedure from CD / DVD
   Start rescue procedure from USB mass storage

     Use the ↑ and ↓ keys to select which entry is highlighted.
     Press enter to boot the selected OS, 'e' to edit the
     commands before booting, or 'c' for a command-line.
```

Figure 11-8 mGuard centerport boot menu

3. Then select one of the options to perform the rescue procedure with the arrow keys ↓ or ↑:
   Start rescue procedure via DHCP/BootP+TFTP
   OR
   Start rescue procedure from CD/DVD
   OR
   Start rescue procedure from USB mass storage
   To apply the selection, press the **Enter** key.
   The options include:

Start rescue procedure via DHCP/BootP+TFTP

Effect: The mGuard downloads all necessary files from the TFTP server. The names of the downloaded files correspond to those used from the other models of the mGuard family, with the following exceptions:

– install.p7s -> install.x86_64.p7s
– jffs2.img.p7s -> firmware.img.x86_64.p7s

In the case of the file install.x86_64.p7s, ensure that the file version that Innominate has declared for use for the rescue procedure via TFTP is used.

Start rescue procedure from CD/DVDs

Requirement: The firmware of the mGuard has been previously burnt to CD - see below under “Burning mGuard firmware to CD-ROM” on page 212.

Effect: The mGuard downloads all necessary files from the inserted CD.

With this in mind, while the boot menu is displayed and before applying this selection, insert the CD with the mGuard firmware into the CD drive.

(For security reasons, the mGuard centerport does not boot from the CD).

Start rescue procedure from USB mass storage

Requirement: The firmware of the mGuard has been previously copied to a USB storage medium (USB stick).

As the first primary partition, the USB storage medium must have a VFAT file system and must contain the same files in the same folders, as stored on the CD. In addition to this, as is the case for a CD, the specified files can be located in the **Rescue Config** folder.

Effect: The mGuard downloads all necessary files from the connected USB storage medium. With this in mind, while the boot menu is displayed and before applying this selection at the very latest, connect the USB storage medium containing the firmware to the USB interface. (For security reasons, the mGuard centerport does not boot from the USB storage medium).

4. Once the rescue procedure is complete, a corresponding message appears on the monitor. Follow any further on-screen instructions.

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 206):

Burning mGuard firmware to CD-ROM

The firmware for the mGuard can be burnt to CD. A zip file is available for download from the download page of www.innominate.com.

The content of this zip archive can be burnt as a data CD. The following files must be located in the following folders/under the following path names on the CD:

– Firmware/install.x86_64.p7s

- Firmware/firmware.img.x86_64.p7s

In the case of the file install.x86_64.p7s, ensure that the file version that Innominate has declared for use for the rescue procedure via CD is used.

If required, these files can be made available in the **Rescue Config** folder on the CD:

Rescue Config/licence.lic	License file that should be installed in the device during the rescue procedure.
Rescue Config/<serial>.lic	As above, only the wildcard <serial> is replaced by the serial number of the device. The same CD can be used for various devices simultaneously.
Rescue Config/preconfig.atv	Configuration profile, which should be applied in the firmware during the rescue procedure. The file must be applied by script Rescue Config/preconfig.sh.
Rescue Config/<serial>.atv	Same as <serial>.lic
Rescue Config/preconfig.sh	Script file, which is run directly after installation of the new firmware. You can find details in the document “Innominate mGuard - Application Note: Rollout Support” under www.innominate.com.

11.9 Technical data

Hardware properties	
Platform	Multi-core x86 processor architecture
Network interfaces	1 LAN port I 1 WAN port Ethernet IEEE 802.3 10/100/1000 Base TX I RJ45 I full/half duplex I auto MDIX
Other interfaces	VGA console I 2 x serial RS-232, D-SUB 9 connector I 6 x USB
Drives	1 HDD I 1 DVD-RW
Redundancy options	Depending on the firmware used
Power supply	2 x 100 V AC ... 240 V AC, 250 W at 50/60 Hz, redundant
Power consumption	Dependent on the expansion stage
Humidity range	20% ... 90% during operation, non-condensing 10% ... 90% out of service
Degree of protection	Front IP20
Temperature range	0°C ... +50°C (operation) -20°C ... +70°C (storage)
Dimensions (H x W x D)	88 x 482 x 472 mm (2 HE x 19“ x 18.58“)
Weight	10 kg

Firmware and power values	
Firmware compatibility	mGuard 7.1 or later: Innominate recommends using the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	2000 Mbps bidirectional I 2000 Mbps bidirectional
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	600 Mbps bidirectional
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (1 x Power, 1 x HDD) I Boot menu I Log File I Remote Syslog

Other	
Conformance	CE, developed according to UL requirements

12 mGuard industrial rs

Table 12-1 Available mGuard industrial rs versions

Available versions	Order No.
mGuard industrial rs	HW-105000
mGuard industrial rs Analog	HW-105010
mGuard industrial rs ISDN	HW-105020
mGuard industrial rs VPN	BD-501000
mGuard industrial rs VPN Analog	BD-501010
mGuard industrial rs VPN ISDN	BD-501020

The **mGuard industrial rs** can be used as a firewall/VPN router via Ethernet or via serial dial-up connections. It is available in three device versions:

- With integrated modem
- With integrated ISDN terminal adapter
- Without these devices

The **mGuard industrial rs** is suitable for secure remote services (remote diagnostics, remote configuration). The device is designed for standard DIN rail mounting and is therefore ideal for use in industrial applications.

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

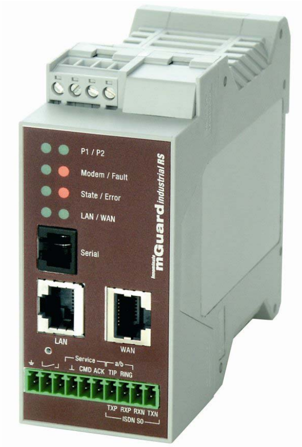
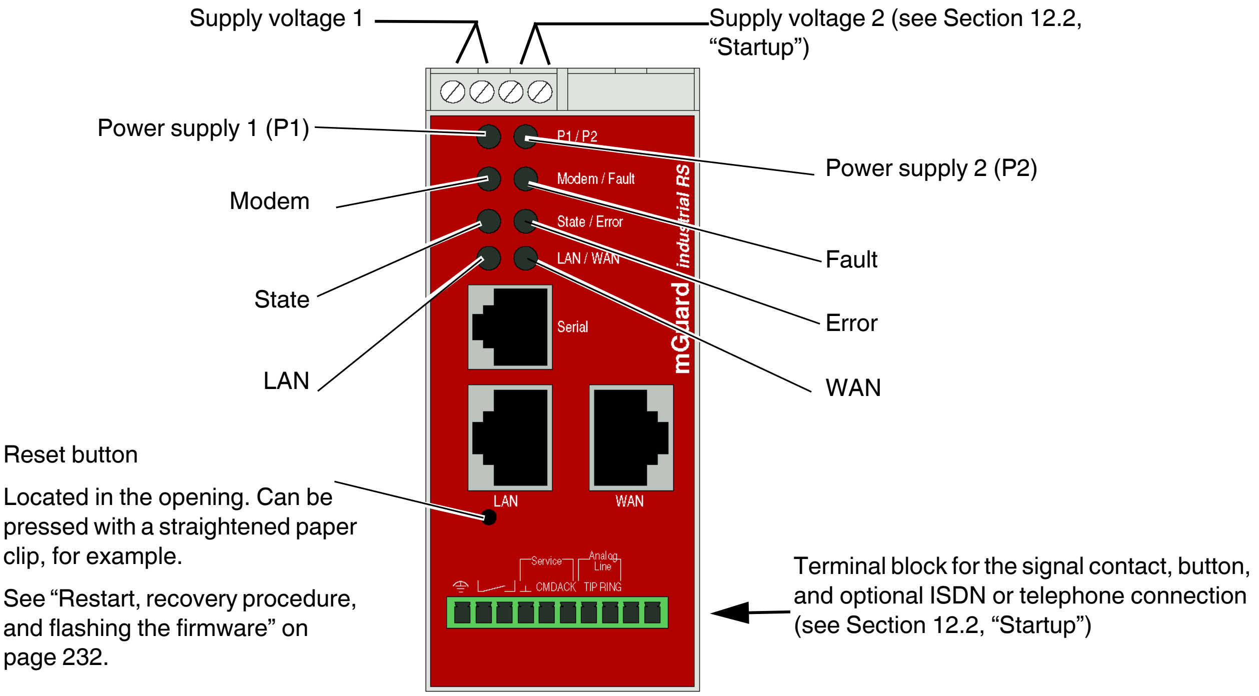


Figure 12-1 mGuard industrial rs

12.1 Operating elements and LEDs



Reset button

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

See “Restart, recovery procedure, and flashing the firmware” on page 232.

Terminal block for the signal contact, button, and optional ISDN or telephone connection (see Section 12.2, “Startup”)

Figure 12-2 Operating elements and LEDs on the mGuard industrial rs

Table 12-2 LEDs on the mGuard industrial 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 (see “Signal contact” on page 222). (The signal contact is interrupted during a restart.)
State	Green	Flashing	**Heartbeat**. The device is correctly connected and operating.
Error	Red	Flashing	**System error**. Restart the device. – Press the Reset button (for 1.5 seconds). – Alternatively, briefly disconnect the device power supply and then connect it again. If the error is still present, start the recovery procedure (see “Performing a recovery procedure” on page 233) or contact your dealer.
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 LED 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	

12.2 Startup

12.2.1 Safety notes

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

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

General notes regarding usage

> **NOTE: Select suitable ambient conditions**
> - Ambient temperature:
>   0°C ... +55°C
> - Maximum humidity, non-condensing:
>   10% ... 95%
>
> To avoid overheating, do not expose the mGuard to direct sunlight or other heat sources.

> **NOTE: Cleaning**
> Clean the device housing with a soft cloth. Do not use aggressive solvents.

12.2.2 Checking the scope of supply

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

The scope of supply includes:

- mGuard industrial rs
- Package slip
- Terminal block for the power supply connection (inserted)
- Terminal block for the signal contact, button, and an optional ISDN or telephone connection
- 2 cover caps for RJ45 sockets

12.3 Installation of mGuard industrial rs

⚠ **WARNING:** The housing must not be opened.

⚠ **WARNING:** The shielding 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; in this case, the operator may be required to implement appropriate measures. When installed in residential or office areas, the mGuard industrial rs may only be operated in control cabinets with fire protection properties according to EN 60950-1.

12.3.1 Mounting/removal

Mounting

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

- Pull out the terminal block from the bottom of the mGuard industrial rs and wire the signal lines and other connections as required (see “Connection options on the lower terminal block” on page 220).
- Tighten the screws on the screw terminal blocks with at least 0.22 Nm.

  Wait to insert the terminal block base.
- Mount the mGuard industrial 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.

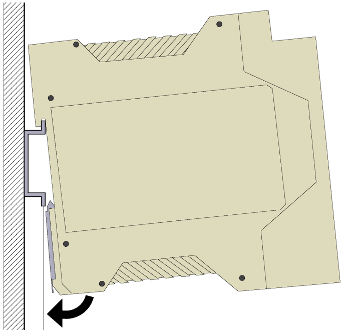


Figure 12-3 Mounting the mGuard industrial rs on a DIN rail

- Attach the top snap-on foot of the mGuard industrial rs to the DIN rail and then press the mGuard industrial rs down towards the DIN rail until 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 219).
- Make any necessary network connections at the LAN port or WAN port (see “Connecting to the network” on page 219).
- Connect the corresponding device at the Serial port as required (see “Serial port” on page 223).

Removal

- Remove or disconnect the connections.

- To remove the mGuard industrial rs from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the mGuard industrial rs.

12.3.2 Connecting the supply voltage

> **WARNING:** The mGuard industrial 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.

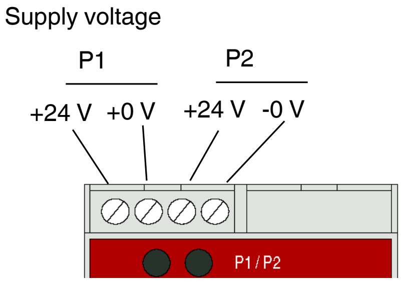


Figure 12-4 Supply voltage

Supply voltage

- – NEC Class 2 power source 12 V DC or 24 V DC
- – -25% ... +33% Safety Extra Low Voltage (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 mGuard industrial rs alone. The supply voltage is electrically isolated from the housing.

If the supply voltage is not redundant, the mGuard industrial 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.

12.3.3 Connecting to the network

> **WARNING:** Only connect the mGuard network ports to LAN installations.
>
> When connecting to the network, use cables with bend protection on the plugs.
>
> Cover unused sockets with the dust protection caps provided.
>
> Some telecommunications connections also use RJ45 sockets; these must not be connected to the RJ45 sockets of the mGuard.

LAN port

- Connect the local computer or the local network to the LAN port of the mGuard using a UTP Ethernet cable (CAT5).

If your computer is already connected to a network, patch the mGuard between the existing network connection.

Please note that configuration can only be completed via the LAN interface and that the firewall of the mGuard industrial rs blocks all IP data traffic from the WAN to the LAN interface.

WAN port

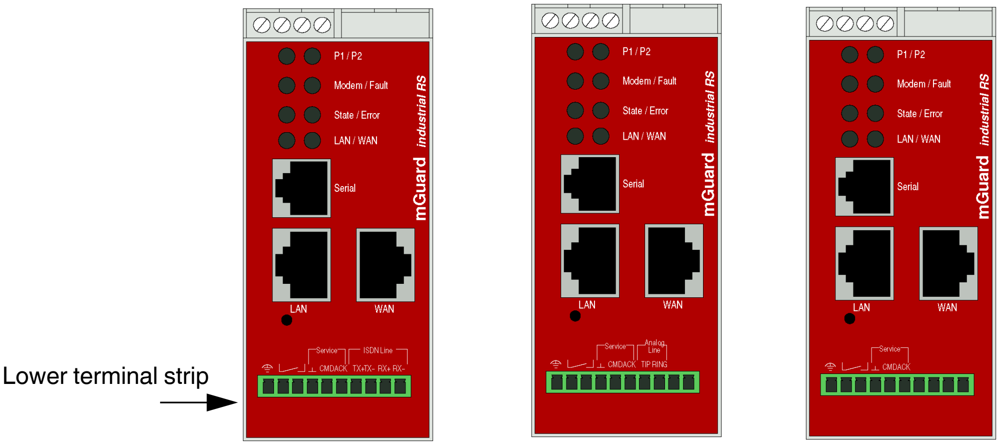
- Use a UTP cable (CAT5).
- Connect the external network via the WAN socket, e.g., WAN, Internet. (Connections to the remote device/network are established via this network.)

Driver installation is not required.

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

Connection options on the lower terminal block

The mGuard industrial rs is available in three versions, which can be distinguished by the connection options on the lower terminal strip:



With ISDN terminal With analog modem WITHOUT modem/ISDN

Figure 12-5 mGuard industrial rs: Lower terminal strip

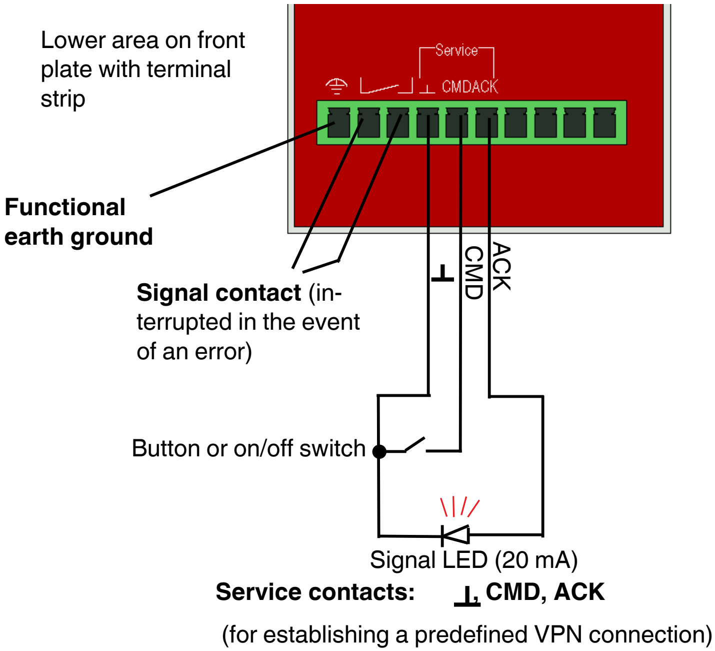

Lower area on front plate with terminal strip
Service
CMD ACK
Functional earth ground
Signal contact (interrupted in the event of an error)
⊥
CMD
ACK
Button or on/off switch
Signal LED (20 mA)
Service contacts: ⊥, CMD, ACK
(for establishing a predefined VPN connection)

Figure 12-6 mGuard industrial rs: **Without** modem/ISDN terminal adapter

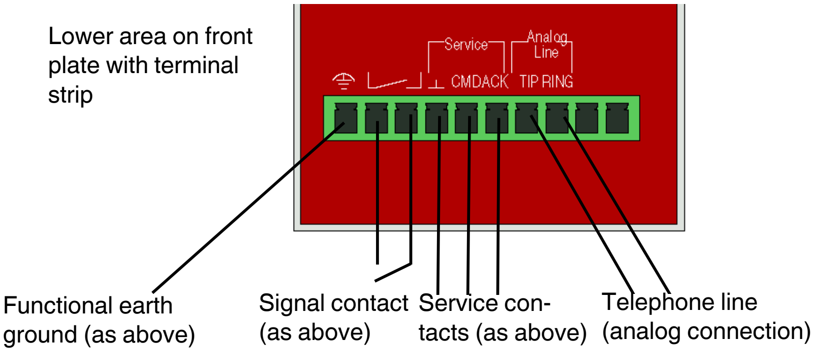

Lower area on front plate with terminal strip
Service
Analog Line
CMD ACK
TIP RING
Functional earth ground (as above)
Signal contact (as above)
Service contacts (as above)
Telephone line (analog connection)

Figure 12-7 mGuard industrial rs **with modem**

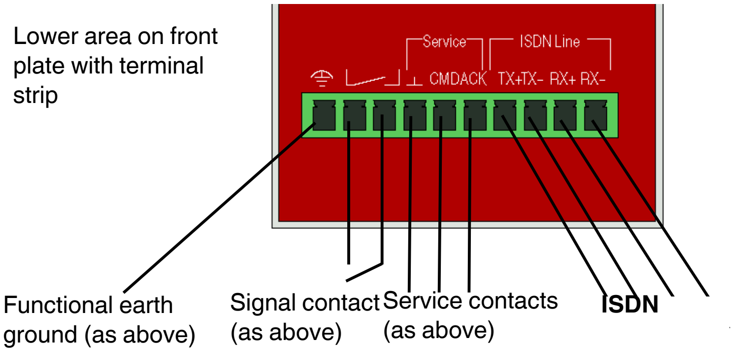

Lower area on front plate with terminal strip
Service
ISDN Line
CMD ACK
TX+ TX- RX+ RX-
Functional earth ground (as above)
Signal contact (as above)
Service contacts (as above)
ISDN

Figure 12-8 mGuard industrial 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 mGuard industrial rs. The mGuard industrial 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 mGuard industrial 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 mGuard industrial 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 mGuard industrial 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 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) must not be connected to an external voltage source; they should always be connected as described here.

A **push 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 12-6 to Figure 12-8).

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 (in the web interface under “IPsec VPN >> Global >> Options”).

Operating a connected button

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

  Flashing indicates that the 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. Only 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 illuminated, 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 mGuard industrial rs as a device in the ISDN network. The table below describes the assignment of the contacts to 8-pos. connections both for plugs and for sockets, for example RJ45:

Table 12-3 Assignment of the contacts to 8-pos. connections

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

In the case of direct connection to an ISDN-NTBA, the mGuard connections must be established as follows:

NTBA a1 -----> mGuard Pin 9 (Rx+)

NTBA a2 -----> mGuard Pin 7 (Tx+)

NTBA b1 -----> mGuard Pin 10 (Rx-)

NTBA b2 -----> mGuard Pin 8 (Tx-)

Serial port

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

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

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

- A PC is connected directly to the serial interface of the mGuard (via the serial interface of the PC). The PC user can then use a terminal program to configure the mGuard via the command line.
- Or a modem is connected to the serial interface of the 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 connection to the mGuard and configure it via a web browser.

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

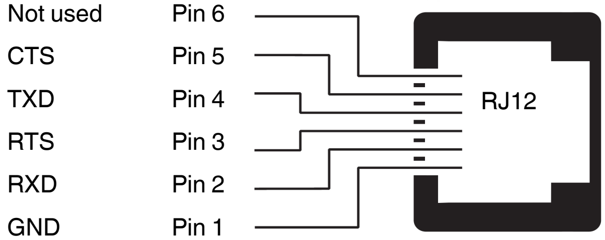


Figure 12-9 Pin assignment of the RJ12 socket (serial port)

On the mGuard industrial 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.

12.4 Preparing the configuration

12.4.1 Connection requirements

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

12.4.2 Local configuration on startup (EIS)

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

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

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

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

Table 12-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard industrial rs	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (in the web interface under “Network >> Interfaces >> General”). Alternatively, you can select a different stealth configuration or use another network mode.

If inconsistencies are no longer detected, a message appears indicating that a valid IP address has been set.

- Click on “Next”.

12.5 Configuration in Stealth mode

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

- https://192.168.1.1/ (see page 227)
- https://1.1.1.1/ (see page 227)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 228).

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

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

12.5.1 IP address 192.168.1.1

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

– The mGuard is in the delivery state.

– The mGuard was reset to the default settings via the web interface and restarted.

– The rescue procedure (flashing of the mGuard) or the recovery procedure has been performed.

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

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

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

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

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

12.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the 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 and if the default gateway can be accessed via the WAN port of the mGuard at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 229). 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

12.5.3 Assigning the IP address via BootP

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

For IP address assignment, the 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.

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

Notes for BootP

During initial startup, the mGuard transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the mGuard no longer sends BootP requests. The FL MGUARD can then no longer be accessed via IP address 192.168.1.1.

After receiving a BootP reply, the mGuard no longer sends BootP requests, not even after it has been restarted. For the 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 mGuard is connected to a computer using a Microsoft Windows operating system.

12.6 Establishing a local configuration connection

Web-based administrator interface

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

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

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

Table 12-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard industrial rs	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

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

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

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 12-5).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the Recovery procedure (see “Performing a recovery procedure” on page 233).

If the administrator web page is not displayed

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

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 225).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

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

  Click on “Properties” under “LAN settings”.

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

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

After successful connection establishment

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

Explanation:

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

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

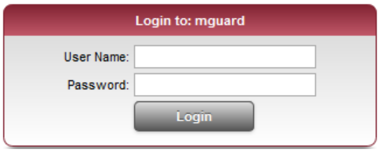


Figure 12-10 Login

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

User Name:	admin
Password:	mGuard

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

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

12.7 Remote configuration

Requirement

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

The option for remote configuration is disabled by default.

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

How to proceed

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

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

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

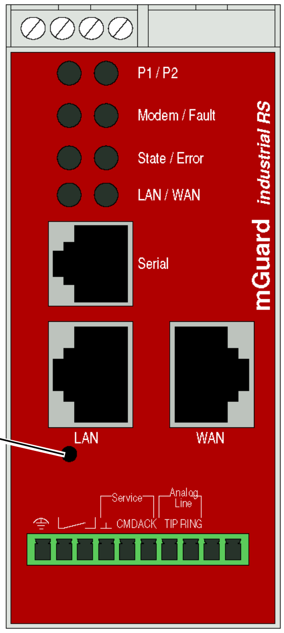
Configuration

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

12.8 Restart, recovery procedure, and flashing the firmware

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

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



Reset button

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

Figure 12-11 Reset button

12.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

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

12.8.2 Performing a recovery procedure

Objective

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 mGuard.

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

Table 12-6 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
mGuard industrial rs	Stealth	https://1.1.1.1/	https://192.168.1.1/

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

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

Possible reasons for performing the recovery procedure:

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

> Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.
>
> You can find application notes under the following Internet address: www.innominate.com.

Action

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

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

12.8.3 Flashing the firmware/rescue procedure

Objective

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

- **All configured settings are deleted.** The mGuard is set to the delivery state.
- In Version 5.0.0 or later of the mGuard, the licenses installed on the mGuard are retained after flashing the firmware. Therefore, they do not have to be installed again.
- For the mGuard industrial rs, only firmware version 5.1.0 or later can be installed.

Possible reasons

The administrator and root password have been lost.

Requirements

NOTE: To flash the firmware, a DHCP and TFTP server or a BootP and TFTP server must be installed on the locally connected computer.

Install the DHCP and TFTP server, if necessary (see “Installing the DHCP and TFTP server” on page 258).

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

Action

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

- Hold down the Reset button until the State, LAN, and WAN LEDs light up green. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The State LED flashes.

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

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

  The Modem, State, and LAN LEDs form a running light.

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

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

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.
- As soon as the procedure is complete, the Modem, State, and LAN LEDs flash green simultaneously.
- Restart the mGuard. To do this, briefly press the **Reset button**.

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 229).

12.9 Technical data

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 RJ45 I full duplex I auto MDIX
Other interfaces	Serial RS-232, RJ11 socket I Optional analog modem I optional ISDN-TA
Drives	–
Redundancy options	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, non-condensing
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	mGuard v5.0 or later: Innominate recommends firmware version 6.x or 7.x to be used with the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	99 Mbps bidirectional I 99 Mbps bidirectional
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	70 Mbps bidirectional
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central 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

13 EAGLE mGuard

Table 13-1 Available EAGLE mGuard versions

Available versions	Order No.
EAGLE mGuard	HW-201000
EAGLE mGuard VPN	BD-301010

The **EAGLE mGuard** is designed for DIN rail mounting (according to DIN EN 60715) and is therefore ideal for use in industrial applications.

The optional configuration connection and option to establish a phone dial-up connection via the RS-232 interface open up a wealth of applications.

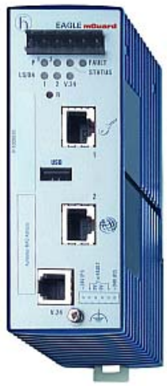


Figure 13-1 EAGLE mGuard

13.1 Operating elements and LEDs

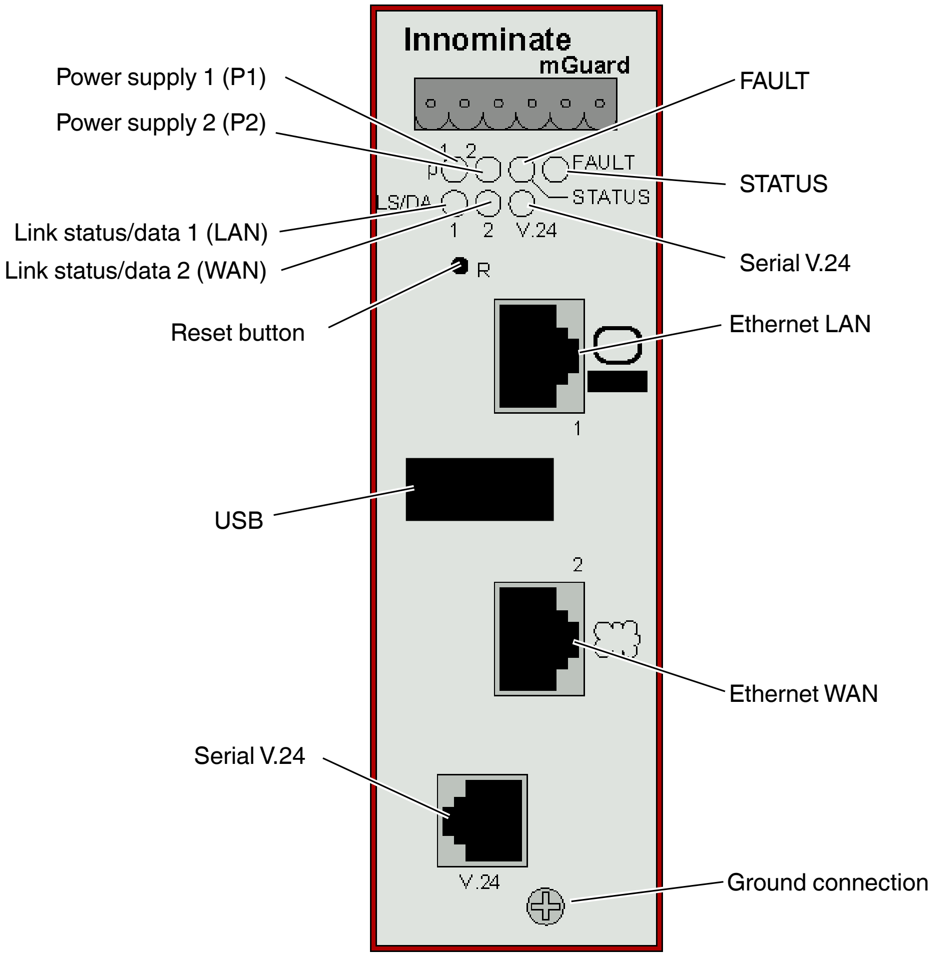


Figure 13-2 Operating elements and LEDs on the EAGLE mGuard

Table 13-2 LEDs on the EAGLE mGuard

LED	State		Meaning
P1, P2	Green	On	**Power supply 1 or 2 is active.**
STATUS	Green	On	The mGuard is ready.
		Flash-ing	The mGuard is starting.
FAULT	Red	On	The signal contact is open due to an error (see “Signal contact” on page 241).
LS/DA 1/2 V.24	Green	On	**Link present**
	Yel-low	Flash-ing	Data transfer

13.2 Startup

13.2.1 Safety notes

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

NOTE: Risk of material damage due to incorrect wiring

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

General notes regarding usage

NOTE: Select suitable ambient conditions

- Ambient temperature:
  0°C ... +60°C
- Maximum humidity, non-condensing:
  10% ... 95%

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

NOTE: Cleaning

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

13.2.2 Checking the scope of supply

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

The scope of supply includes:

- EAGLE mGuard
- Package slip

13.3 Installation of EAGLE mGuard

WARNING: The housing must not be opened.

WARNING: This is a Class A item of equipment. This equipment can cause radio interference in residential areas; in this case, the operator may be required to implement appropriate measures. When installed in residential or office areas, the EAGLE mGuard may only be operated in control cabinets with fire protection properties according to EN 60950-1.

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

Connecting the voltage supply and signal contact

Terminal block

The connection of the supply voltage and the signal contact is established via a 6-pos. terminal block.

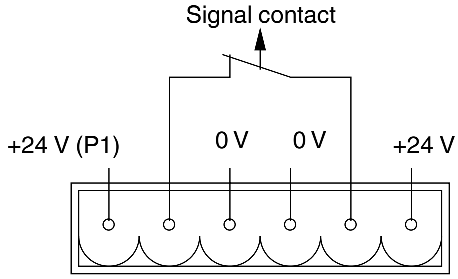


Figure 13-3 Terminal block base

WARNING: The EAGLE mGuard is designed for SELV operation. Therefore, only PELV circuits or optionally SELV circuits with voltage limitations according to EN 60950-1 may be connected to the supply voltage connections and the signal contact.

The EAGLE mGuard can be operated at a DC voltage of 9.6 ... 60 V DC, max. 1 A optionally at an AC voltage of 18 ... 30 V AC, max. 1 A. Use the +24 V and 0 V pins to connect the AC voltage.

Operating voltage

- NEC Class 2 power source 12 V DC or 24 V DC, -25% +33%
- Safety Extra Low Voltage (SELV/PELV, redundant inputs isolated)
- Max. 5 A. Buffer time min. 10 ms 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 EAGLE mGuard alone.

The supply voltage is electrically isolated from the housing.

Startup

- Start up the EAGLE mGuard with the connection of the supply voltage via the 6-pos. terminal block.
- Lock the terminal block with the lateral locking screw.

Signal contact

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

The signal contact monitors the EAGLE mGuard 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.
- Permanent error in the EAGLE mGuard (internal 3.3 V DC voltage, supply voltage 1 or 2 < 9.6 V, etc.).
- A faulty link status of at least one port. The link status message for each port can be masked on the EAGLE mGuard via the management software.

  By default upon delivery, there is no connection monitoring.
- Error during selftest.

If the supply voltage is not redundant, the EAGLE mGuard indicates the failure of the supply voltage. This message can be prevented by feeding the supply voltage via both inputs.

Ground connection

- To ground the EAGLE mGuard, a separate screw connection is available.

Serial port

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

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

To configure the mGuard via the serial interface. There are two options:

- A PC is connected directly to the serial interface of the mGuard (via the serial interface of the PC). The PC user can then use a terminal program to configure the mGuard via the command line.
- Or a modem is connected to the serial interface of the 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 connection to the mGuard and configure it via a web browser.

To manage data traffic via the serial interface instead of via the WAN interface of the mGuard. In this case, a modem should be connected to the serial interface.

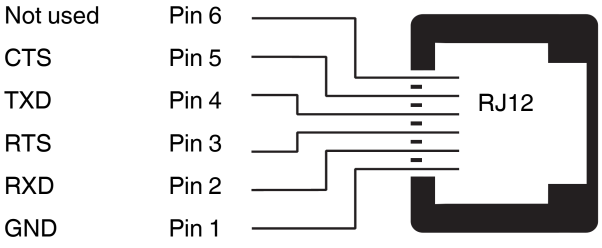


Figure 13-4 Pin assignment of the RJ12 socket (serial port)

Mounting

The device is ready to operate when it is supplied. The recommended sequence for mounting is as follows:

- Pull out the terminal block from the EAGLE mGuard and wire the supply voltage lines and signal lines.
- Mount the EAGLE mGuard on a grounded 35 mm DIN rail according to EN 60715.

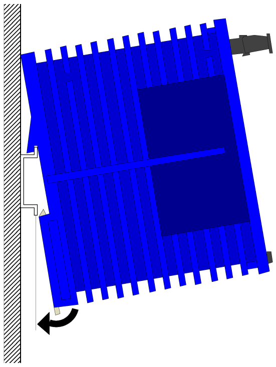


Figure 13-5 EAGLE mGuard: DIN rail mounting

- Attach the top snap-on foot of the EAGLE mGuard to the DIN rail and then press the EAGLE mGuard down towards the DIN rail until it engages with a click.
- Connect the device to the local network or the local computer to be protected (LAN).
- Via the socket for connection to the external network, establish the connection to the external network, e.g., Internet. Connections to the remote device or network are established via this network.
- The front plate of the EAGLE mGuard housing is grounded via the ground connection.

Network connection

NOTE: If your computer is already connected to a network, patch the EAGLE mGuard between the existing network connection.

Please note that configuration can only be completed via the LAN interface and that the firewall of the EAGLE mGuard blocks 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.

Both network interfaces of the EAGLE mGuard are configured for connection on a computer.

When connecting to a **hub**, please note the following:

When auto negotiation is deactivated, the Auto MDIX function is also deactivated. This means that the port of the EAGLE mGuard must either be connected to the uplink port of the hub or connected to the hub using a cross-link cable.

Removal

To remove the EAGLE mGuard from the DIN rail, insert a screwdriver horizontally in the locking slide under the housing, pull it down – without tilting the screwdriver – and then pull up the EAGLE mGuard.

13.4 Preparing the configuration

13.4.1 Connection requirements

- The EAGLE mGuard must be connected to at least one active power supply unit.
- **For local configuration**: The computer used for configuration:
  - Must be connected to the LAN socket of the mGuard
  - Or the computer must be connected to the mGuard via the network.
- **For remote configuration**: The mGuard must be configured so that remote configuration is permitted.
- The mGuard must be connected, i.e., the required connections must be working.

13.4.2 Local configuration on startup (EIS)

As of firmware version 7.2, initial startup of mGuard products provided in Stealth mode is considerably easier. From this version onwards, the EIS (Easy Initial Setup) procedure enables startup to be performed via preset or user-defined management addresses without actually having to connect to an external network.

The mGuard is configured using a web browser on the computer used for configuration.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

According to the default setting, the mGuard can be accessed via the following addresses:

Table 13-3 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
EAGLE mGuard	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is preset to the “multiple Clients” stealth configuration. You need to configure a management IP address and default gateway if you want to use VPN connections (in the web interface under “Network >> Interfaces >> General”). Alternatively, you can select a different stealth configuration or use another network mode.

13.5 Configuration in Stealth mode

On initial startup, the mGuard can be accessed via two addresses:

- https://192.168.1.1/ (see Page 245)
- https://1.1.1.1/ (see Page 245)

Alternatively, an IP address can be assigned via BootP (see “Assigning the IP address via BootP” on page 246).

The mGuard can be accessed via https://192.168.1.1/ if the external network interface is not connected on startup.

Computers can access the mGuard via https://1.1.1.1/ if they are directly or indirectly connected to the LAN port of the mGuard. For this purpose, the 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.

13.5.1 IP address 192.168.1.1

In Stealth mode, the mGuard can be accessed via the LAN interface via IP address 192.168.1.1 within network 192.168.1.0/24, if one of the following conditions applies.

– The mGuard is in the delivery state.
– The mGuard was reset to the default settings via the web interface and restarted.
– The rescue procedure (flashing of the mGuard) or the recovery procedure has been performed.

To access the configuration interface, it may be necessary to adapt the network configuration of your computer.

Under **Windows 7**, proceed as follows:

- In the Control Panel, open the “Network and Sharing Center”.
- Click on “LAN connection”. (The “LAN connection” item is only displayed if a connection exists from the LAN interface on the computer to a mGuard in operation or another partner).
- Click on “Properties”.
- Select the menu item “Internet protocol Version 4 (TCP/IPv4)”.
- Click on “Properties”.
- First select “Use the following IP address” under “Internet Protocol Version 4 Properties”, then enter the following address, for example:

IP address:	192.168.1.2
Subnet mask:	255.255.255.0
Default gateway:	192.168.1.1

Depending on the configuration of the mGuard, it may then be necessary to adapt the network interface of the locally connected computer or network accordingly.

13.5.2 IP address https://1.1.1.1/

With a configured network interface

In order for the 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 and if the default gateway can be accessed via the WAN port of the mGuard at the same time.

In this case, the web browser establishes a connection to the mGuard configuration interface after the address https://1.1.1.1/ is entered (see “Establishing a local configuration connection” on page 247). Continue from this point.

After access via IP address 1.1.1.1, the FL MGUARD can no longer be accessed via IP address 192.168.1.1

13.5.3 Assigning the IP address via BootP

After assigning an IP address via BootP, the FL MGUARD can no longer be accessed via IP address 192.168.1.1

For IP address assignment, the 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.

Section 14.1 explains IP address assignment using the free Windows software “IP Assignment Tool” (IPAssign.exe).

Notes for BootP

During initial startup, the mGuard transmits BootP requests without interruption until it receives a valid IP address. After receiving a valid IP address, the mGuard no longer sends BootP requests. The product can then no longer be accessed via IP address 192.168.1.1.

After receiving a BootP reply, the mGuard no longer sends BootP requests, not even after it has been restarted. For the 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 mGuard is connected to a computer using a Microsoft Windows operating system.

13.6 Establishing a local configuration connection

Web-based administrator interface

The mGuard is configured via a web browser that is executed on the configuration computer.

NOTE: The web browser used must support SSL encryption (i.e., HTTPS).

The mGuard can be accessed via one of the following addresses:

Table 13-4 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
EAGLE mGuard	Stealth	https://1.1.1.1/	https://192.168.1.1/

Proceed as follows:

- Start a web browser.
- Make sure that the browser, when it is started, does not automatically establish a connection as otherwise the connection establishment to the mGuard may be more difficult.

In **Internet Explorer**, make the following settings:

- In the “Tools” menu, select “Internet Options” and click on the “Connections” tab:
- Under “Dial-up and Virtual Private Network settings”, select “Never dial a connection”.
- Enter the address of the mGuard completely into the address line of the web browser (refer to Table 13-4).

You access the administrator website of the mGuard.

If the administrator web page of the mGuard cannot be accessed

If you have forgotten the configured address

If the address of the mGuard in Router, PPPoE or PPTP mode has been set to a different value, and the current address is not known, the mGuard must be reset to the default settings specified above for the IP address using the **Recovery** procedure (see “Performing a recovery procedure” on page 251).

If the administrator web page is not displayed

If the web browser repeatedly reports that the page cannot be displayed, try the following:

- Check whether the default gateway of the connected configuration computer is initialized (see “Local configuration on startup (EIS)” on page 243).
- Disable any active firewalls.
- Make sure that the browser does not use a proxy server.

  In **Internet Explorer** (Version 8), make the following settings: “Tools” menu, “Internet Options”, “Connections” tab.

  Click on “Properties” under “LAN settings”.

  Check that “Use a proxy server for your LAN” (under “Proxy server”) is not activated in the “Local Area Network (LAN) Settings” dialog box.
- If other LAN connections are active on the computer, deactivate them until the configuration has been completed.

  Under the Windows menu “Start, Settings, Control Panel, Network Connections” or “Network and Dial-up Connections”, right-click on the corresponding icon and select “Disable” in the context menu.

After successful connection establishment

Once a connection has been established successfully, a security alert may be displayed.

Explanation:

As administrative tasks can only be performed using encrypted access, a self-signed certificate is supplied with the device.

- Click “Yes” to acknowledge the security alert.

The login window is displayed.

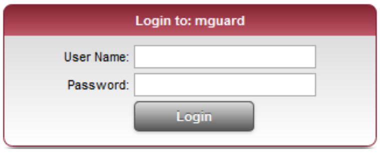


Figure 13-6 Login

- To log in, enter the preset user name and password (please note these settings are case-sensitive):

User Name:	admin
Password:	mGuard

The mGuard can then be configured via the web interface. For additional information, please refer to the software reference manual.

For security reasons, we recommend you change the default root and administrator passwords during initial configuration.

13.7 Remote configuration

Requirement

The mGuard must be configured so that remote configuration is permitted.

The option for remote configuration is disabled by default.

Switch on the remote configuration option in the web interface under “Management >> Web Settings”.

How to proceed

To configure the mGuard via its web user interface from a remote computer, establish the connection to the mGuard from there.

Proceed as follows:

- Start the web browser on the remote computer.
- Under address, enter the IP address where the mGuard can be accessed externally over the Internet or WAN, together with the port number (if required).

Example

If the mGuard can be accessed over the Internet, for example, via address https://123.45.67.89/ and port number 443 has been specified for remote access, the following address must be entered in the web browser of the remote peer:
https://123.45.67.89/

If a different port number is used, it should be entered after the IP address, e.g.,
https://123.45.67.89:442/

Configuration

The mGuard can then be configured via the web interface. For additional information, please refer to the software reference manual.

13.8 Restart, recovery procedure, and flashing the firmware

The Reset button is used to set the device to one of the following states:

- Performing a restart
- Performing a recovery procedure
- Flashing the firmware/rescue procedure

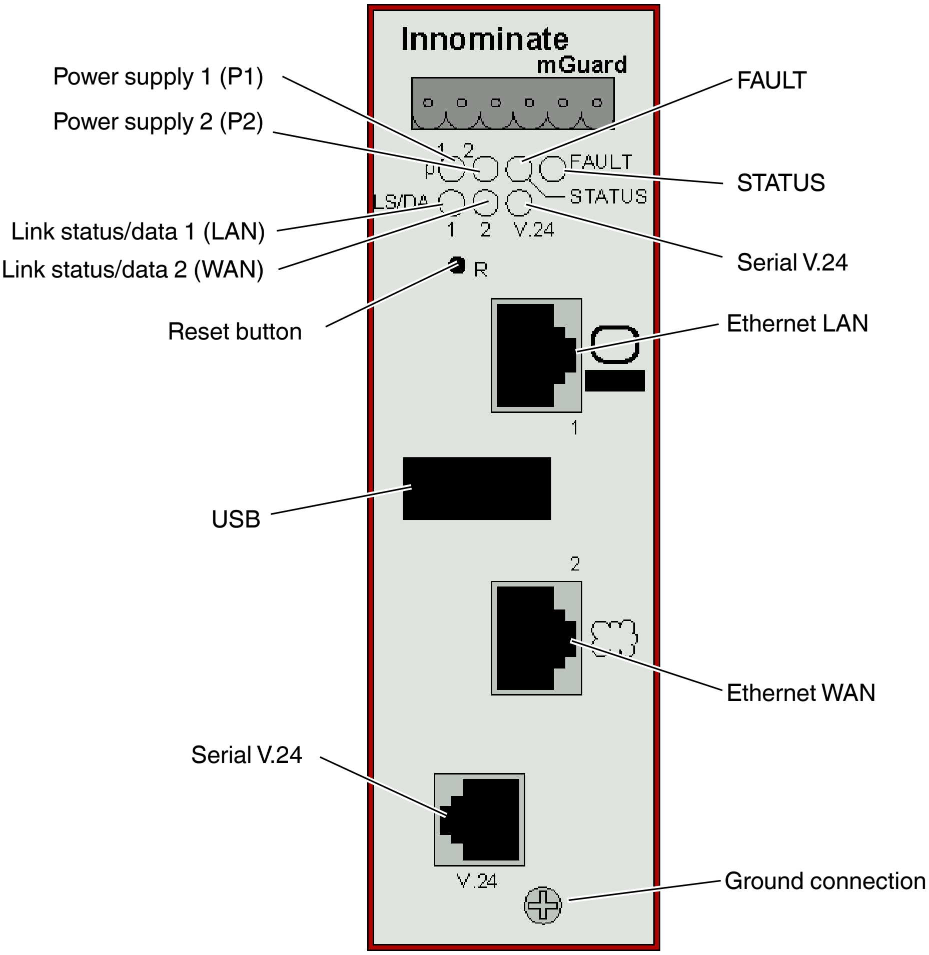


Figure 13-7 Reset button

13.8.1 Performing a restart

Objective

The device is restarted with the configured settings.

Action

- Press the Reset button for around 1.5 seconds until the middle LED lights up in red. (Alternatively, disconnect the power supply and then connect it again.)

13.8.2 Performing a recovery procedure

Objective

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 mGuard.

When performing the recovery procedure, the default settings are established:

Table 13-5 Preset addresses

Default setting	Network mode	Management IP #1	Management IP #2
EAGLE mGuard	Stealth	https://1.1.1.1/	https://192.168.1.1/

The mGuard is reset to Stealth mode with the default setting “multiple Clients”.

- The CIFS integrity monitoring function is also disabled because this only works when the management IP is active.
- In addition, MAU management is switched on for Ethernet connections. HTTPS access is enabled via the local Ethernet connection (LAN).
- The settings configured for VPN connections and the firewall are retained, including passwords.

Possible reasons for performing the recovery procedure:

- The mGuard is in Router or PPPoE mode.
- The configured device address of the mGuard differs from the default setting.
- The current IP address of the device is not known.

Up-to-date information on the recovery and flashing procedure can be found in the application note for your mGuard firmware version.

You can find application notes under the following Internet address: www.innominate.com.

Action

- Slowly press the **Reset button** six times.
  After approximately 2 seconds, the STATUS LED lights up yellow.
- Press the **Reset button** slowly again six times.
  If successful, the STATUS LED lights up yellow.
  If unsuccessful, the FAULT LED lights up red.

If successful, the device restarts after two seconds and switches to Stealth mode. The device can then be reached again under the corresponding addresses.

13.8.3 Flashing the firmware/rescue procedure

Objective

The entire firmware of the mGuard should be reloaded on the device.

- **All configured settings are deleted.** The mGuard is set to the delivery state.
- In Version 5.0.0 or later of the mGuard, the licenses installed on the mGuard are retained after flashing the firmware. Therefore, they do not have to be installed again.

Possible reasons

The administrator and root password have been lost.

Requirements

NOTE: To flash the firmware, a DHCP and TFTP server or a BootP and TFTP server must be installed on the locally connected computer.

Install the DHCP and TFTP server, if necessary (see “Technical data” on page 253).

NOTE: Installing a second DHCP server in a network could affect the configuration of the entire network.

Action

NOTE: Do not interrupt the power supply to the mGuard during any stage of the flashing procedure. Otherwise, the device could be damaged and may have to be reactivated by the manufacturer.

- Hold down the Reset button until the 1, 2, and V.24 LEDs light up. Then, the mGuard is in the recovery state.
- **Release the Reset button within a second of entering the recovery state.**

  If the Reset button is not released, the mGuard is restarted.

  The mGuard now starts the recovery system: It searches for a DHCP server via the LAN interface in order to obtain an IP address.

  The 1, 2, and V.24 LEDs light up orange.

  The “install.p7s” file is loaded from the TFTP server or SD card. It contains the electronically signed control procedure for the installation process. Only files that are signed are executed.

  The control procedure deletes the current contents of the Flash memory and prepares for a new firmware installation.

  The 1, 2, and V.24 LEDs form a running light.

  The “jffs2.img.p7s” firmware file is downloaded from the TFTP server or SD card and written to the Flash memory. This file contains the actual mGuard operating system and is signed electronically. Only files signed by Innominate are accepted.

  This process takes around 3 to 5 minutes. The 1, 2, and V.24 LEDs are off, the P1, P2, and STATUS LEDs light up continuously green.

  The new firmware is extracted and configured. This procedure takes 1 to 3 minutes.
- As soon as the procedure is complete, the 1, 2, and V.24 LEDs flash green simultaneously.
- Restart the mGuard. To do this, briefly press the **Reset button**.

The mGuard is in the delivery state. You can now configure it again (see “Establishing a local configuration connection” on page 247):

13.9 Technical data

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 RJ45 I full duplex I auto MDIX I Optional 100 Base FX (F0)
Other interfaces	Serial RS-232, RJ11 socket I USB
Drives	–
Redundancy options	Depending on the firmware used
Power supply	24 V DC I max. 300 mA I PELV/SELV I redundant I -25% ... +25% voltage range
Power consumption	max. 7.2 W at 24 V
Humidity range	10% ... 95% during operation, non-condensing
Degree of protection	IP20
Temperature range	0°C ... +60°C (operation) -40°C ... +80°C (storage)
Dimensions (H x W x D)	131 x 47 x 111 mm
Weight	340 g

Firmware and power values	
Firmware compatibility	mGuard v5.0 or later: Innominate recommends firmware version 6.x or 7.x to be used with the latest patch releases; For the scope of functions, please refer to the relevant firmware data sheet.
Data throughput (router I firewall)	99 Mbps bidirectional I 99 Mbps bidirectional
Hardware-based encryption	DES I 3DES I AES-128/192/256
Encrypted VPN throughput (AES-256)	70 Mbps bidirectional
Management support	Web GUI (HTTPS) I command line interface (SSH) I SNMP v1/2/3 I central device management software
Diagnostics	LEDs (P1, P2, Status, Fault, LAN, WAN, V.24) I signal contact (24 V, 1 A) I Log File I Remote Syslog

Other	
Conformance	CE I FCC I UL 508 I GL

14 Assigning IP addresses and setting up DHCP/TFTP servers

14.1 Assigning the IP address using IPAssign.exe

Step 1: Downloading and executing the program

- On the Internet, select the link www.innominate.com/downloads.
- The BootP IP addressing tool from Innominate can be found under “Software & Misc”.
- Double-click on the “IPAssign_mGuard.exe” file.
- In the window that opens, click on “Run”.

Step 2: “IP Assignment Tool”

The program opens and the start screen of the addressing tool appears.

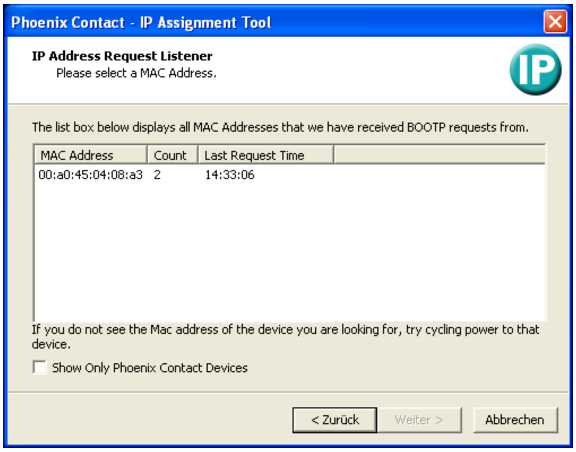
The program is mainly in English. However, the program buttons change according to the country-specific settings.

The start screen displays the IP address of the PC. This helps when addressing the mGuard in the subsequent steps.

- Click on “Next”.

Step 3: “IP Address Request Listener”

All devices sending a BootP request are listed in the window which opens. These devices are waiting for a new IP address.



Phoenix Contact - IP Assignment Tool

IP Address Request Listener

Please select a MAC Address.

The list box below displays all MAC Addresses that we have received BOOTP requests from.

MAC Address	Count	Last Request Time
00:a0:45:04:08:a3	2	14:33:06

If you do not see the Mac address of the device you are looking for, try cycling power to that device.

□ Show Only Phoenix Contact Devices

Figure 14-1 “IP Address Request Listener” window

In this example, the mGuard has MAC ID 00.A0.45.04.08.A3.

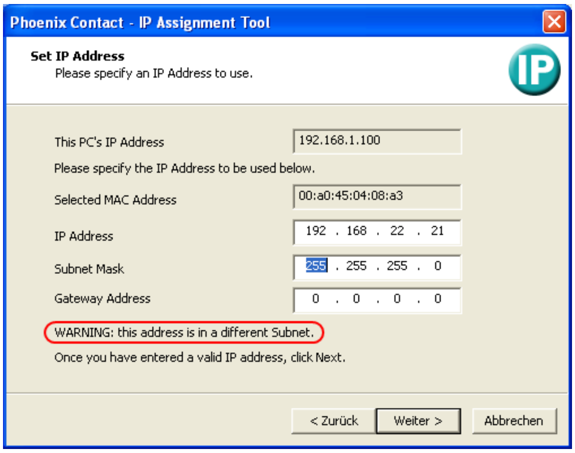
- Select the device to which you would like to assign an IP address.
- Click on “Next”.

Step 4: “Set IP address”

The following information is displayed in the window which opens:

– IP address of the PC

- MAC address of the selected device
- IP parameters of the selected device (IP address, subnet mask, and gateway address)
- Any incorrect settings


Phoenix Contact - IP Assignment Tool

Set IP Address
Please specify an IP Address to use.

This PC's IP Address: 192.168.1.100

Please specify the IP Address to be used below.

Selected MAC Address: 00:a0:45:04:08:a3

IP Address: 192 . 168 . 22 . 21

Subnet Mask: 255 . 255 . 255 . 0

Gateway Address: 0 . 0 . 0 . 0

WARNING: this address is in a different Subnet.

Once you have entered a valid IP address, click Next.

Figure 14-2 “Set IP Address” window with incorrect settings

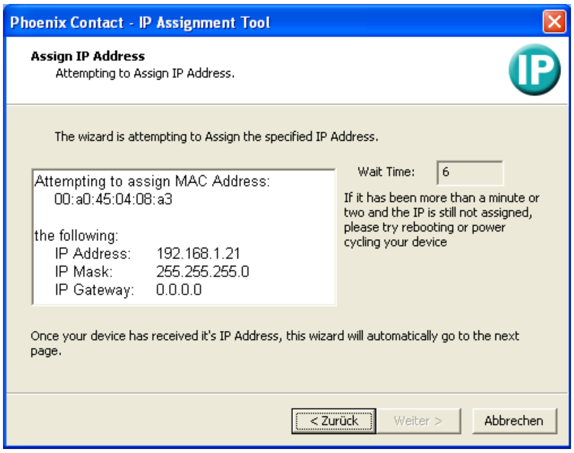
- Adjust the IP parameters according to your requirements.

If inconsistencies are no longer detected, a message appears indicating that a valid IP address has been set.

- Click on “Next”.

Step 5: “Assign IP address”

The program attempts to transmit the IP parameters set to the mGuard.


Phoenix Contact - IP Assignment Tool

Assign IP Address
Attempting to Assign IP Address.

The wizard is attempting to Assign the specified IP Address.

```
Attempting to assign MAC Address:
   00:a0:45:04:08:a3

the following:
   IP Address:     192.168.1.21
   IP Mask:        255.255.255.0
   IP Gateway:     0.0.0.0
```

Wait Time: 6

If it has been more than a minute or two and the IP is still not assigned, please try rebooting or power cycling your device

Once your device has received it's IP Address, this wizard will automatically go to the next page.

Figure 14-3 “Assign IP address” window

Following successful transmission, the next window opens.

Step 6: Finishing IP address assignment

The window that opens informs you that address assignment has been successfully completed. It gives an overview of the IP parameters that have been transmitted to the device with the MAC address shown.

To assign IP parameters for additional devices:

- Click on “Back”.

To exit IP address assignment:

- Click on “Finish”.

If required, the IP parameters set here can be changed on the mGuard web interface under “Network >> Interfaces”.

14.2 Installing the DHCP and TFTP server

Installing a second DHCP server in a network could affect the configuration of the entire network.

Under Windows

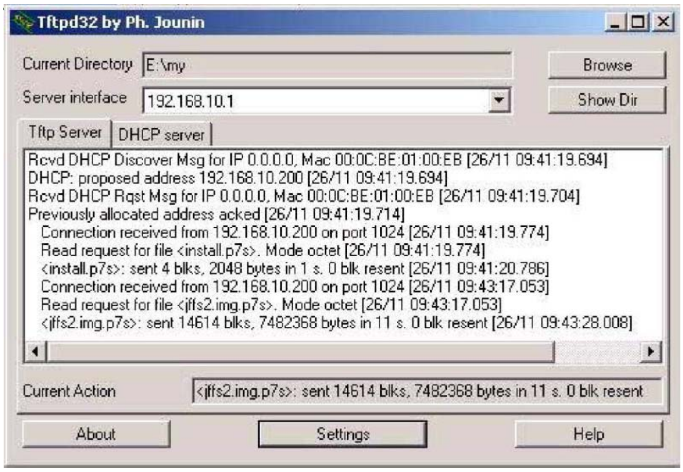
Install the program provided in the download area at www.innominate.com .

- 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 mGuard image files are saved: **install.p7s, jffs2.img.p7s**
- If a major release upgrade of the firmware is carried out by flashing, the license file purchased for the upgrade must also be stored here under the name **licence.lic**.

  Make sure that this is the correct license file for the device (under “Management >> Update” on the web interface).



Current Directory: E:\my

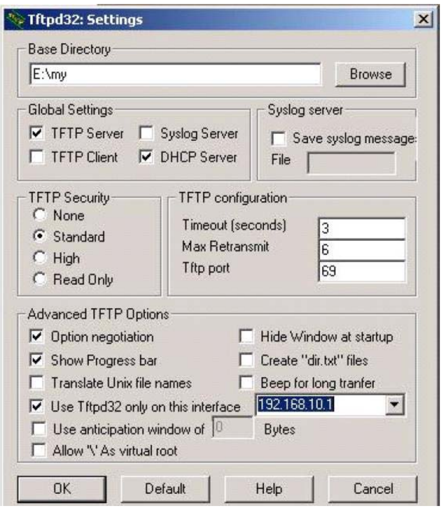
Server interface: 192.168.10.1

```
Rcvd DHCP Discover Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.694]
DHCP: proposed address 192.168.10.200 [26/11 09:41:19.694]
Rcvd DHCP Rqst Msg for IP 0.0.0.0, Mac 00:0C:BE:01:00:EB [26/11 09:41:19.704]
Previously allocated address acked [26/11 09:41:19.714]
  Connection received from 192.168.10.200 on port 1024 [26/11 09:41:19.774]
  Read request for file <install.p7s>. Mode octet [26/11 09:41:19.774]
  <install.p7s>: sent 4 blks, 2048 bytes in 1 s. 0 blk resent [26/11 09:41:20.786]
  Connection received from 192.168.10.200 on port 1024 [26/11 09:43:17.053]
  Read request for file <jffs2.img.p7s>. Mode octet [26/11 09:43:17.053]
  <jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent [26/11 09:43:28.008]
```

Current Action: <jffs2.img.p7s>: sent 14614 blks, 7482368 bytes in 11 s. 0 blk resent

Figure 14-4 Entering the host IP

- Switch to the “TFTP Server” or “DHCP Server” tab page and click on “Settings” to set the parameters as follows:



Base Directory: E:\my

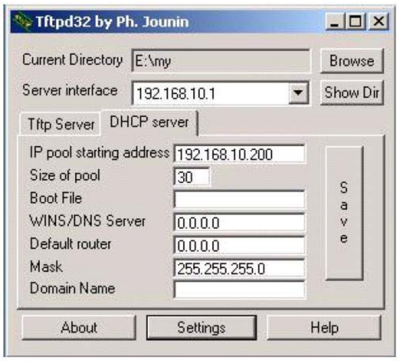
Global Settings: ☑ TFTP Server □ Syslog Server □ TFTP Client ☑ DHCP Server

Syslog server: □ Save syslog message File

TFTP Security: ○ None ● Standard ○ High ○ Read Only

TFTP configuration: Timeout (seconds) 3 Max Retransmit 6 Tftp port 69

Advanced TFTP Options:
☑ Option negotiation □ Hide Window at startup
☑ Show Progress bar □ Create "dir.txt" files
□ Translate Unix file names □ Beep for long tranfer
☑ Use Tftpd32 only on this interface 192.168.10.1
□ Use anticipation window of 0 Bytes
□ Allow '\' As virtual root



Current Directory: E:\my

Server interface: 192.168.10.1

IP pool starting address: 192.168.10.200
Size of pool: 30
Boot File:
WINS/DNS Server: 0.0.0.0
Default router: 0.0.0.0
Mask: 255.255.255.0
Domain Name:

Figure 14-5 Settings

Under Linux

All current Linux distributions include DHCP and TFTP servers.

- Install the corresponding packages according to the instructions provided for the relevant distribution.
- Configure the DHCP server by making the following settings in the **/etc/dhcpd.conf** file:

```
subnet 192.168.134.0 netmask 255.255.255.0 {
range 192.168.134.100 192.168.134.119;
option routers 192.168.134.1;
option subnet mask 255.255.255.0;
option broadcast address 192.168.134.255;}
```

This example configuration provides 20 IP addresses (.100 to .119). It is assumed that the DHCP server has the address 192.168.134.1 (settings for ISC DHCP 2.0).

The required TFTP server is configured in the following file: **/etc/inetd.conf**

- In this file, insert the corresponding line or set the necessary parameters for the TFTP service. (Directory for data: **/tftpboot)**

```
tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/
```

The mGuard image files must be saved in the **/tftpboot** directory:
install.p7s, jffs2.img.p7s

- If a major release upgrade of the firmware is carried out by flashing, the license file purchased for the upgrade must also be stored here under the name **licence.lic**.

  Make sure that this is the correct license file for the device (under “Management >> Update” on the web interface).
- Then restart the inetd process to apply the configuration changes.
- When using a different mechanism, e.g., xinetd, please consult the relevant documentation.