

# User Manual

## Industrial ETHERNET Firewall EAGLE mGuard

# User Manual

## Industrial ETHERNET Firewall EAGLE mGuard

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2006 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly guaranteed in the contract. This publication has been created by Hirschmann Automation and Control GmbH according to the best of our knowledge. Hirschmann reserves the right to change the contents of this manual without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the details in this publication.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

Printed in Germany (21.9.06)

Hirschmann Automation and Control GmbH  
Stuttgarter Straße 45-51  
72654 Neckartenzlingen  
Tel. +49 1805 141538 -01-0806

# Table of Contents

<b>1</b>	<b>Introduction.....</b>	<b>6</b>
	Network features .....	6
	Firewall features.....	6
	Anti-Virus features.....	6
	VPN features .....	6
	Additional features .....	7
	Support .....	7
1.1	Device versions .....	7
	mGuard smart.....	7
	mGuard PCI.....	7
	mGuard blade .....	7
	EAGLE mGuard.....	8
	mGuard delta .....	8
<b>2</b>	<b>Typical application scenarios.....</b>	<b>9</b>
	Transparent Mode .....	9
	Network Router .....	9
	DMZ .....	9
	VPN Gateway.....	10
	WLAN over VPN.....	10
	Solving Network Conflicts.....	11
<b>3</b>	<b>Control and LEDs.....</b>	<b>12</b>
3.1	mGuard blade .....	12
3.2	mGuard delta .....	13
3.3	EAGLE mGuard .....	14
3.4	mGuard smart .....	15
3.5	mGuard PCI .....	16
<b>4</b>	<b>Startup .....</b>	<b>17</b>
4.1	Package contents .....	18
	Included in the package.....	18
4.2	Connect the mGuard blade .....	19
	Installing mGuard bladeBase .....	19
	Installing mGuard blade .....	19
	Control Unit (CTRL Slot) .....	19
	Connecting mGuard blade.....	20
4.3	Connect the mGuard delta .....	21
4.4	Connect the EAGLE mGuard .....	22
	Terminal block .....	22
	Assembly .....	22
	Startup procedure .....	23
	Network connection .....	23
	Dismantling .....	23
4.5	Connect the mGuard smart .....	24
4.6	Connect the mGuard PCI .....	25
	4.6.1 Choice between Driver mode or Power-over-PCI mode .....	25
	Driver Mode .....	25
	Power-over-PCI Mode .....	26
	4.6.2 Hardware installation .....	28
	4.6.3 Driver installation .....	29
	Windows XP .....	29
	Windows 2000.....	30
	Linux .....	33
<b>5</b>	<b>Configuration preparation.....</b>	<b>34</b>

5.1	Connecting the mGuard .....	34
	mGuard blade .....	34
	mGuard delta .....	34
	EAGLE mGuard .....	34
	mGuard smart .....	34
	mGuard PCI .....	34
5.2	Local Configuration: At startup .....	34
5.2.1	EAGLE mGuard .....	35
	With a configured network interface .....	35
	Without a configured network interface .....	35
	Entering the IP parameter via HiDiscovery .....	36
5.2.2	mGuard blade and mGuard smart .....	37
	With a configured network interface .....	37
	Without a configured network interface .....	37
5.2.3	mGuard delta .....	38
5.2.4	mGuard PCI .....	39
	Install the mGuard PCI Card .....	39
	Install the mGuard PCI Driver .....	39
	Configure the Network Interface .....	39
	The Default Gateway .....	40
5.3	Setting Up a Local Configuration Connection .....	41
	Web-based Administrator interface .....	41
	After a connection has been successfully setup .....	42
	Configuring the device .....	43
5.4	Remote Configuration .....	43
	Prerequisite .....	43
	Remote configuration .....	43
<b>6</b>	<b>Configuration .....</b>	<b>44</b>
6.1	Operation .....	44
6.2	Menu Basic Settings .....	46
6.2.1	Basic Settings → System .....	46
	Host .....	46
	Signal contact (only EAGLE mGuard) .....	48
	Time and Date .....	49
	Shell Access .....	50
6.2.2	Basic Settings → Network Interfaces .....	52
	General .....	52
	Network Mode → Transparent (factory setting except mGuard delta) .....	55
	Network Mode → Router (factory setting mGuard delta) .....	56
	Network Mode → PPPoE .....	59
	Network Mode → PPTP .....	59
	Network Mode → Router, PPPoE or PPTP .....	60
	Ethernet .....	61
	Serial Port (only mGuard blade, delta and EAGLE mGuard) .....	62
	Hardware .....	64
6.2.3	Basic Settings → Load/Save .....	65
	Load/Save .....	65
	Profiles on the ACA (EAGLE mGuard only) .....	66
6.2.4	Basic Settings → Central Management .....	68
	Configuration Pull .....	68
6.2.5	Basic Settings → Licensing .....	69
	Overview .....	69
	Install .....	70

## Table of Contents

6.2.6	Basic Settings → Update .....	71
	Overview .....	71
	Update .....	72
	AntiVirus Pattern.....	73
6.2.7	Basic Settings → Restart .....	74
6.3	Menu Security .....	75
6.3.1	Security → SNMP .....	75
	Query.....	75
	Trap .....	77
	LLDP.....	78
6.3.2	Security → Web Access .....	79
	General .....	79
	Access.....	79
6.3.3	Security → Local Authentication .....	81
	Passwords.....	81
6.3.4	Security → External Authentication .....	83
	Remote Users .....	83
	Radius Server .....	84
	Status .....	84
6.4	Menu Network Security (not blade controller) .....	85
6.4.1	Network Security → Packet Filter .....	85
	Untrusted Port .....	85
	Trusted Port.....	86
	MAC Filter .....	88
	Advanced.....	89
6.4.2	Network Security → NAT .....	90
	Masquerading.....	90
	Port Forwarding.....	91
	Connection Tracking.....	93
6.4.3	Network Security → DoS .....	94
	Flood Protection.....	94
6.4.4	Network Security → User Firewall .....	95
	User Firewall Templates .....	95
	User Firewall → Define Template .....	96
	General:.....	96
	Template User .....	96
	Firewall Rules .....	97
6.5	Menu IPsec VPN (not blade controller) .....	98
6.5.1	IPsec VPN → Global .....	98
	Machine Certificate.....	98
	DynDNS Monitoring.....	99
6.5.2	IPsec VPN → Connections .....	99
	Connections.....	99
6.5.3	Define a VPN connection .....	100
	General .....	100
	Authentication .....	103
	Firewall.....	105
	IKE Options.....	106
6.5.4	IPsec VPN → L2TP over IPsec .....	108
	L2TP Server .....	108
6.5.5	IPsec VPN → IPsec Status .....	109
6.6	Menu AntiVirus (not on control unit) .....	111

6.6.1	AntiVirus → HTTP .....	111
	Virus Protection.....	111
6.6.2	Web Security → FTP .....	113
	Virus Protection.....	113
6.6.3	AntiVirus → POP3 .....	116
	Virus Protection.....	116
6.6.4	AntiVirus → SMTP .....	119
	Virus Protection.....	119
6.7	Menu redundancy .....	122
6.7.1	Firewall Redundancy .....	122
	Redundancy.....	123
	ICMP Checks .....	124
6.7.2	Layer 2 Redundancy .....	125
	Ring / Network Coupling.....	125
6.8	Menu Diagnosis .....	126
6.8.1	Log → Settings .....	126
	Remote Logging.....	126
6.8.2	Diagnosis → Event logs .....	127
	AntiVirus.....	128
6.8.3	Diagnosis → Support Info .....	130
	Hardware .....	130
	Snapshot .....	130
6.9	Extended .....	131
6.9.1	Extended → DNS .....	131
	DNS Server .....	131
	DynDNS.....	132
6.9.2	Extended → DHCP .....	133
	Trusted/Untrusted DHCP .....	133
6.10	Menu Entry Blade Control (control unit only) .....	137
6.10.1	Blade control → Overview .....	137
6.10.2	Blade control → Blade 01 to 12 .....	138
	Blade in slot #__.....	138
	Configuration .....	138
6.11	CIDR (Classless InterDomain Routing) .....	140
6.12	Network Sketch .....	141
<b>7</b>	<b>The Rescue Button – restart, recovery procedure and to flash the firmware.....</b>	<b>142</b>
7.1	Performing a Restart .....	142
7.2	Performing a Recovery .....	142
7.3	Flashing the firmware .....	143
	Required before the firmware can be flashed: DHCP and TFTP servers .....	145
7.3.1	Installing DHCP and TFTP servers under Windows or Linux .....	146
	Under Windows: .....	146
	Under Linux .....	147
<b>8</b>	<b>Glossary .....</b>	<b>148</b>
	Asymmetrical encryption .....	148
	DES / 3DES.....	148
	AES .....	148
	Client / Server.....	148
	Datagram .....	148
	Default route.....	149
	DynDNS provider .....	149
	IP address .....	150
	IPsec .....	151
	NAT (Network Address Translation).....	151

---

## Table of Contents

Port Number .....	151
PPPoE.....	152
PPTP.....	152
X.509 Certificate .....	152
Protocol, communication protocol .....	152
Proxy .....	152
Service Provider .....	153
Spoofing, Antispoofing .....	153
Symmetrical encryption .....	153
TCP/IP (Transmission Control Protocol/Internet Protocol).....	153
Trap .....	153
VLAN.....	153
VPN (Virtual Private Network).....	154



---

# 1 Introduction

The mGuard protects IP data connections. The device supports the following functions:

- Network Card (mGuard PCI), Switch (mGuard delta)
- VPN router (VPN - Virtual Private Network) for the secure transfer of data via public networks (hardware-based DES, 3DES and AES encryption, IPsec protocol)
- Configurable firewall to provide protection against unauthorized access. The dynamic packet filter inspects the source and destination addresses of data packets and blocks undesired traffic.
- Virus protection with support for the protocols HTTP, FTP, SMTP and POP3.

The device can be conveniently configured using a Web browser.

## Network features

- Transparent (Auto, Static, Multi), Router (Static, DHCP Client), PPPoE (for DSL) and PPTP (for DSL) connectivity
- VLAN
- DHCP server/relay on the external and internal network interfaces
- DNS cache on the internal network interface
- Administration using HTTPS and SSH

## Firewall features

- Stateful packet inspection
- Anti-spoofing
- IP Filtering
- L2 Filtering (only Transparent mode)
- NAT with FTP, IRC and PPTP pass through (only router modes)
- 1:1 NAT (only router modes)
- Port forwarding (only router modes)
- Firewall throughput max. 99MBit/s
- Individual firewall rules for different users (user firewall)

## Anti-Virus features

- ClamAV virus protection
- Supported protocols: HTTP, FTP, POP3 and SMTP (sending)
- The virus filter can decompress the following formats:
  - ZIP
  - RAR
  - GZIP
  - BZIP2
  - TAR
  - MS OLE2
  - MS Cabinet Dateien (CAB)
  - MS CHM (Komprimiertes HTML)
  - MS SZDD
  - UPX
  - FSG
  - Petite

## VPN features

- Protocol: IPsec (Tunnel and Transport Mode)
- IPsec DES encryption - 56 Bit
- IPsec 3DES encryption - 168 Bit
- IPsec AES encryption - 128, 192 and 256 Bit
- Packet authentication: MD5, SHA-1
- Internet Key Exchange (IKE) with Main and Quick Mode
- Authentication: Pre-Shared Key (PSK), X.509v3 certificate
- DynDNS

- NAT-T
- Dead Peer Detection (DPD)
- Hardware encryption
- up to 250 VPN tunnels (please refer to the feature table)
- VPN throughput max. 35MBits/s on 266MHz or 70MBit/s on 533MHz models.
- IPsec firewall and 1:1 NAT
- Default route over VPN

**Additional features**

- MAU management
- Remote logging
- Router/Firewall Redundancy
- IPsec/L2TP Server
- LLDP
- Administration by SNMP v1-v3 (please refer to the feature table) and Innominate Device Manager (IDM)

**Support**

In case of problems with the mGuard please contact your local dealer. Additional information about the device and relevant changes as well as release notes and software updates can be found on the web site:  
 - for the EAGLE mGuard under [www.hirschmann-ac.com](http://www.hirschmann-ac.com),  
 - for all other mGuards under <http://www.innominate.com/>

**1.1 Device versions**

mGuard is available in the following device versions, which have largely identical functions. All devices can be utilised regardless of the processor technology and operating system the connected computers use.

**mGuard smart**

Smallest device model. Can, for example, simply be plugged between the computer or local network (on mGuard's LAN port) and an available router (on mGuard's WAN port), without having to change existing system configurations or driver installations. Designed for instant use in the office or when on the go.



**mGuard PCI**

This card, which can be plugged into a PCI slot, provides the computer it is installed in with all mGuard functions in driver mode and can additionally be utilised as a normal network card. A network card already on hand in the computer or another local computer / local network can be connected in the power-over-PCI mode.



**mGuard blade**

The mGuard blade Pack includes the mGuard bladeBase, which can be easily installed into standard 3 U racks (19 inches) and accommodate up to 12 mGuard blades. Thus this version is ideally suited for use in an industrial environment where it can protect several server systems individually and independently of one another. An additional serial interface enables remote configuration using a telephone dial-up connection or a terminal.

---

## EAGLE mGuard

EAGLE mGuard was developed in cooperation with the Industrial Security Alliance partner Hirschmann Automation and Control GmbH. The device is designed for top hat rail mounting (according to DIN EN 50 022) and is therefore especially suited for use in industrial environments. The optional configuration connection and the option to establish a telephone dial-up connection via the V.24 interface provide for additional applications options.



## mGuard delta

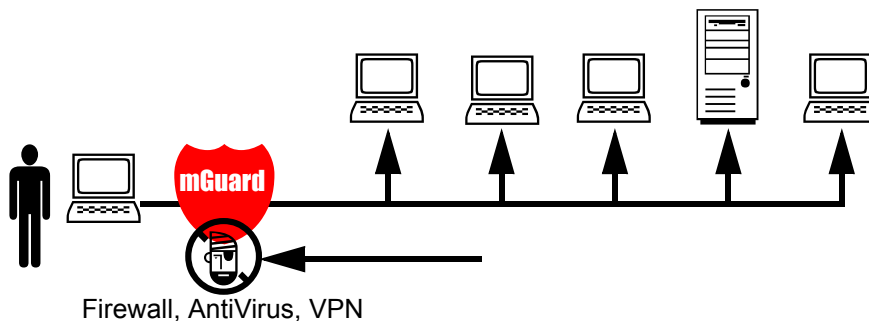
This device model is a compact LAN switch (Ethernet / Fast Ethernet) designed for connecting up to 4 LAN segments. Thus the device is especially suited for logically segmented network environments where the locally connected computers / networks share the mGuard functions. An additional serial interface enables configuration using a telephone dial-up connection or a terminal. With its robust metal housing, mGuard delta is not only suitable as a desktop device but also for placement in wiring closets.



## 2 Typical application scenarios

Some of the more common application scenarios may be found below.

### Transparent Mode

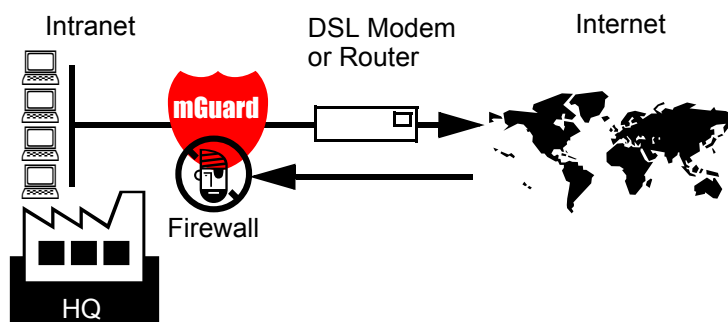


In *Transparent* Mode (factory default) the mGuard can be installed between an individual computer and the rest of the network.

The settings for Firewall, AntiVirus and VPN can be made with a webbrowser at the URL <https://1.1.1.1/>.

On the computer itself no configuration changes are required.

### Network Router



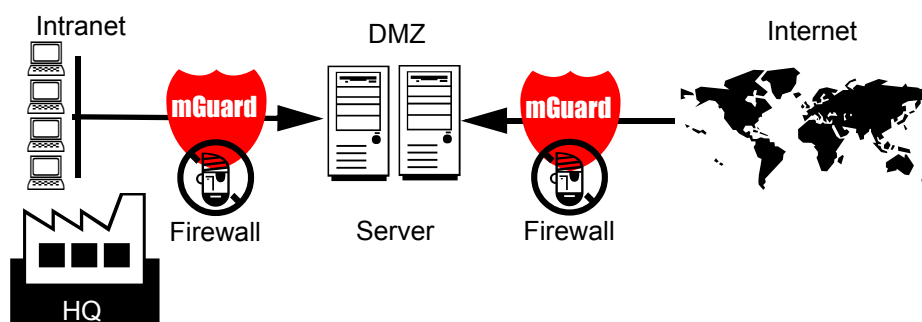
The mGuard is able to provide internet connectivity to a group of computers while protecting the company network with its firewall.

For this purpose one of the following network modes may be used:

- *Router*, if the Internet access is established via a DSL router or dedicated line.
- *PPPoE*, if for example the Internet access is established via a DSL modem using the PPPoE protocol (e.g. in Germany).
- *PPTP*, if for example the Internet access is established via a DSL modem using the PPTP protocol (e.g. in Austria).

The mGuard must be set as the default gateway on the locally connected client system(s).

### DMZ

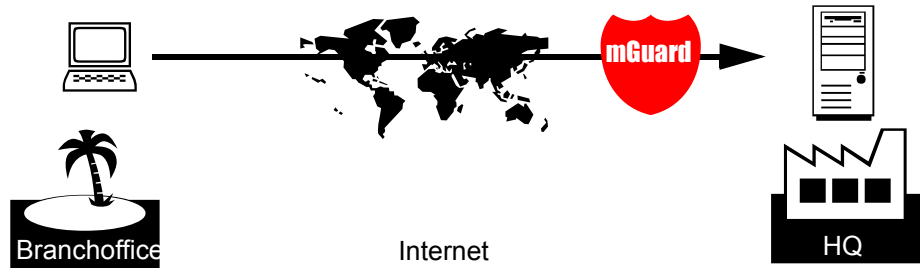


A DMZ (Demilitarized Zone) is a protected network, which sits between an trusted network and untrusted networks. For example a company's website may be inside a DMZ, granting FTP write access to computers in the intranet and HTTP read-only access to both networks.

The IP addresses within the DMZ can be public or private. In the latter case, pub-

lic IPs would be mapped by means of portforwarding to the private addresses within the DMZ.

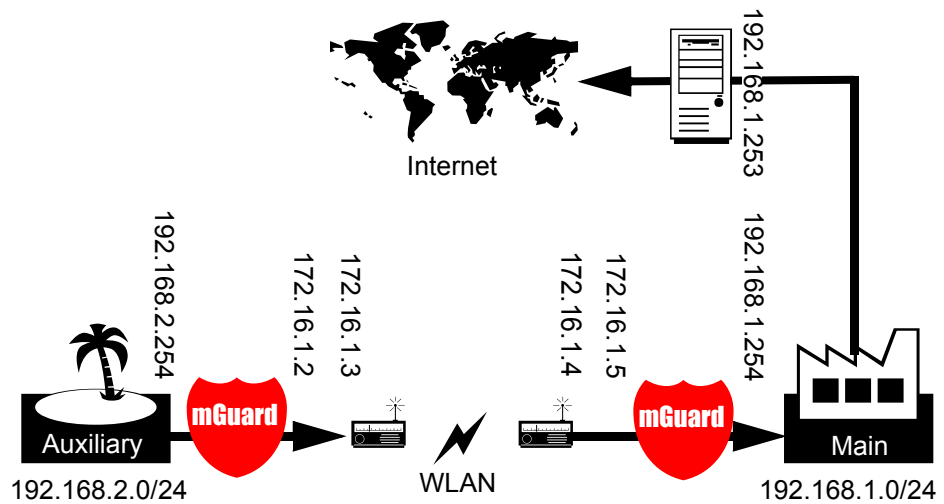
### VPN Gateway



An encrypted access to the company’s network is to be provided to employees at home or in the field. The mGuard thereby provides the services of a VPN gateway.

On the untrusted computers an IPsec capable VPN client must be installed in case the computers operating system does not provide such a service, like Windows 2000 or XP do.

### WLAN over VPN



Two buildings of a company are to be connected with an IPsec protected WLAN connection. From the auxiliary building it shall also be possible to use the main building’s internet connection.

In this example the mGuards were switched into router mode and a separate network with addresses of 172.16.1.x was created for the WLAN. Since the internet should be also available via the VPN from the auxiliary building, a “Default route over VPN” must be configured.

#### Auxiliary building tunnel configuration

Connection type	Tunnel (Net <-> Net)
Local network address	192.168.2.0/24
Remote network address	0.0.0.0/0

In main building the appropriate counterpart to the connection is to be configured:

---

### Main building tunnel configuration

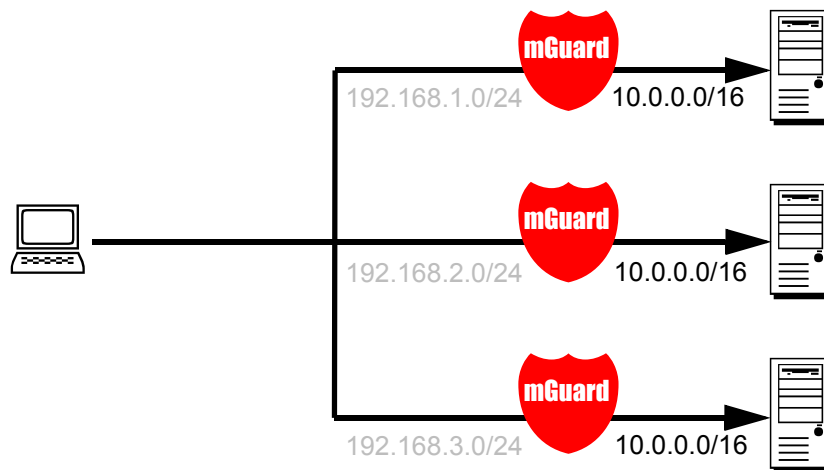
Connection type	Tunnel (Net <-> Net)
Local network address	0.0.0.0/0
Remote network address	192.168.2.0/24

The default route of an mGuard is usually directed over its WAN port. But in this case the internet is reachable via the LAN port:

### Main building default gateway

IP of the default gateway	192.168.1.253
---------------------------	---------------

### Solving Network Conflicts



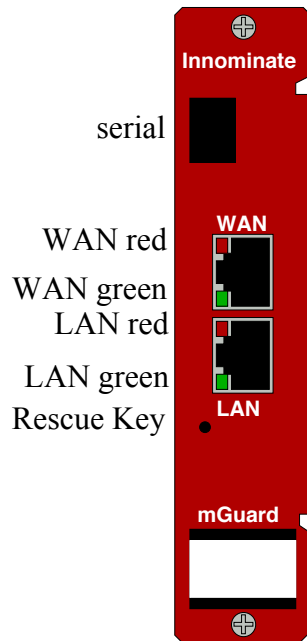
In the illustration above, it is desired that the networks on the right-hand side are accessible from the network or the computer on the left-hand side. For historical or technical reasons, however, the computer networks overlap on the right-hand side.

With the help of mGuards and their 1:1 NAT feature, these networks can be redefined so that the conflict is solved.

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

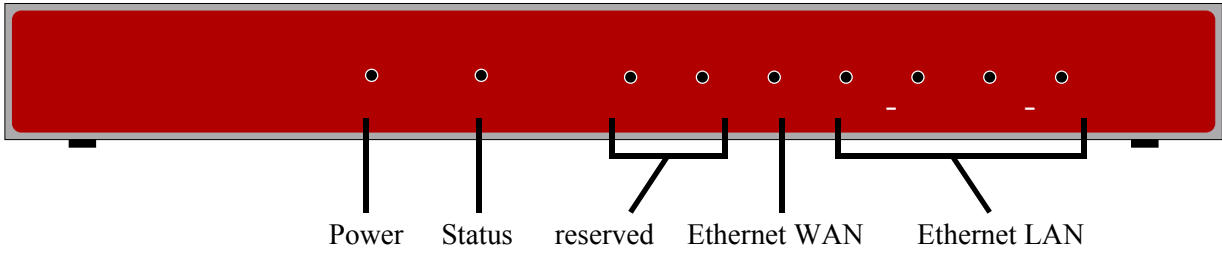
### 3 Control and LEDs

#### 3.1 mGuard blade



LEDs	State	Meaning
<b>WAN Red, LAN Red</b>	flashing	<b>Booting up.</b> After starting or restarting the computer.
<b>WAN Red</b>	flashing	<b>System error.</b> ☒ Perform a system restart. To accomplish this, briefly press the Rescue button (1.5 sec.) If the error occurs again, start the <i>Recovery procedure</i> (see “Performing a Recovery” on page 142) or contact Support.
<b>WAN Green, LAN Green</b>	on or flashing	<b>Ethernet status.</b> Shows the status of the LAN and WAN interface. As soon as the device is connected to the network, the LEDs will be on continuously to indicate that there is a connection. The LEDs will flash when data packets are transferred.
<b>WAN Green, WAN Red, LAN Green</b>	various LED codes	<b>Recovery mode.</b> After pressing the <b>Rescue key</b> See “The Rescue Button – restart, recovery procedure and to flash the firmware” on page 142.

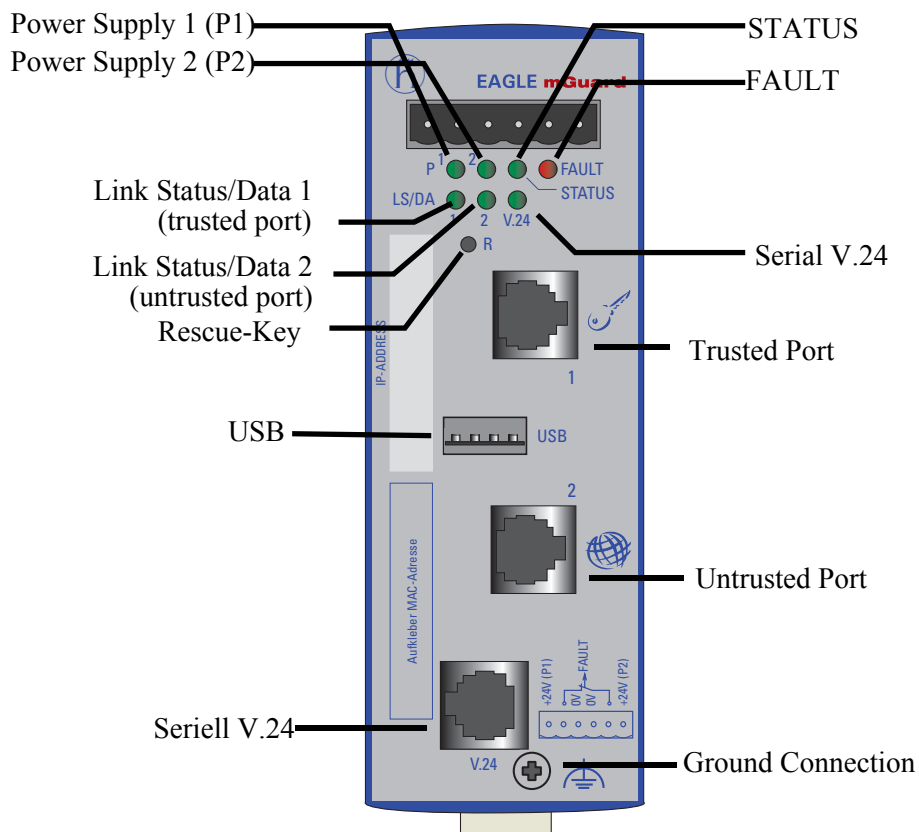
### 3.2 mGuard delta



LEDs	State	Meaning
<b>Power</b>	on	The power supply is active.
<b>Status</b>	on	The mGuard is booting.
	heartbeat (flash, flash, pause, ...)	The mGuard is ready.
<b>1,2</b>	-	Reserved.
<b>3 (WAN)</b>	on	Link detected.
	flashing	Data transfer.
<b>4-7 (LAN)</b>	on	Link detected.
	flashing	Data transfer.

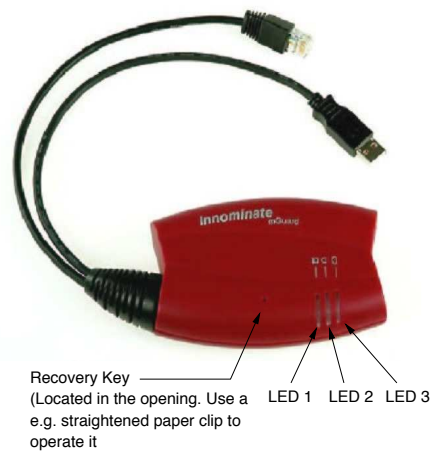


### 3.3 EAGLE mGuard



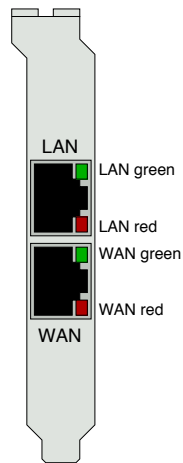
LEDs	State	Meaning
<b>P1, P2</b>	green	The power supply 1 or 2 is active.
<b>STATUS</b>	green blinking	The EAGLE mGuard is booting.
	green	The mGuard is ready.
	yellow blinking slowly	The mGuard is in Router Redundancy Backup mode.
<b>FAULT</b>	red	The signal contact is open in case of an error.
<b>LS/DA 1/2 V.24</b>	green	Link detected.
	green blinking (3 times per period)	The port is disabled.
	yellow flashing	Receiving data.
	running light	Initialization phase after a reset.
<b>Display of ACA function STATUS and V.24</b>	both LEDs blinking simultaneously (slow)	ACA writing process.
	both LEDs blinking simultaneously (slow)	ACA reading process.
	both LEDs blinking alternated (fast)	ACA error.

### 3.4 mGuard smart



LEDs	Colour	State	Meaning
2	Red/Green	red/green flashing	<b>Booting up.</b> After connecting the device to the power supply. After a few seconds, the LED will switch to a heartbeat.
	Green	flashing	<b>Heartbeat.</b> The device is correctly connected and functioning.
	Red	flashing	<b>System error.</b> ☒ Perform a system restart. To accomplish this, briefly press the <b>Rescue key</b> (1.5 sec.) OR Disconnect the device from its power supply briefly and then reconnect it. If the error occurs again, start the <i>Recovery procedure</i> (see “Performing a Recovery” on page 142) or contact Support.
1 and 3	Green	on or flashing	<b>Ethernet status.</b> LED 1 shows the status of the internal interface, LED 3 the status of the external interface. As soon as the device is connected to the interface, the LEDs will be on continuously to indicate that there is a connection to the network. The LEDs will flash when data packets are transferred.
1, 2, 3	various LED codes		<b>Recovery mode.</b> After pressing the <b>Rescue key</b> See “The Rescue Button – restart, recovery procedure and to flash the firmware” on page 142.

### 3.5 mGuard PCI



LEDs	State	Meaning
<b>WAN Red, LAN Red</b>	flashing	<b>Booting up.</b> After starting or restarting the computer.
<b>WAN Red</b>	flashing	<b>System error.</b> ☒ Perform a system restart. To accomplish this, briefly press the <b>Rescue key</b> (1.5 sec.) OR Restart your computer. If the error occurs again, start the <i>Recovery procedure</i> (see “Performing a Recovery” on page 142) or contact Support.
<b>WAN Green, LAN Green</b>	on or flashing	<b>Ethernet status.</b> Shows the status of the LAN and WAN interface. As soon as the device is connected to the network, the LEDs will be on continuously to indicate that there is a connection. The LEDs will flash when data packets are transferred.
<b>WAN Green, WAN Red, LAN Green</b>	various LED codes	<b>Recovery mode.</b> After pressing the <b>Rescue key</b> See “The Rescue Button – restart, recovery procedure and to flash the firmware” on page 142.

---

## 4 Startup

**Safety instructions** The mGuard is intended for (protective) low voltage operation. Only connect the mGuard's network interfaces to LAN installations. Some telephone lines also use RJ45 jacks. The mGuard may not be operated on a telephone line.



**Warning mGuard PCI!** Before handling the mGuard PCI, touch the bare metal case of your PC to discharge static electricity from your body.



**Warning!** This is a Class A device. It may cause radio interference in a living area, in which case, the operator may be requested to take appropriate measures.

### General notes regarding usage

- mGuard PCI: Your PC must provide a free PCI slot (3.3V or 5V).
- Use a soft cloth to clean the case of the device. Do not use any aggressive solvents!
- Environmental conditions:  
0 to +40°C (blade, smart) 55°C (PCI) 60° (EAGLE)  
max. 90% (EAGLE: 95%), non-condensing humidity
- To avoid overheating, do not leave it in direct sunlight or expose it to any other source of heat.
- Do not bend the cables sharply. Only use network cables to connect to a network.

### Steps for starting up the device

To startup the device, perform the following steps in the order listed:

Step	Objectives	Page
1	Check the package contents and read the Release Notes	“Package contents” on page 18
2	Connect the Device	<ul style="list-style-type: none"><li>• “Connect the mGuard blade” on page 19</li><li>• “Connect the mGuard delta” on page 21</li><li>• “Connect the EAGLE mGuard” on page 22</li><li>• “Connect the mGuard smart” on page 24</li><li>• “Connect the mGuard PCI” on page 25</li></ul>
3	Configure the device to the extent necessary. To accomplish this, select from the various options offered in the mGuard's configuration menus. For more information regarding which options and settings are required (or desirable) for your operating environment, please read the relevant sections in this manual.	“Local Configuration: At startup” on page 34