Packungsbeilage // mGuard pci² Produktfamilie

mGuard pci² SD	Bestellnummer:	HW-102061
mGuard pci² SD VPN	Bestellnummer:	BD-111040
mGuard pci² SD HT VPN	Bestellnummer:	BD-111070
mGuard pcie² SD	Bestellnummer:	HW-102071
mGuard pcie² SD VPN	Bestellnummer:	BD-111060

DE Einbauanweisung für den Elektroinstallateur

Herzlichen Dank für Ihr Vertrauen in die mGuard Produktfamilie. mGuard pci² ist eine kompakte, PCI-kompatible Firewall/Router/VPN-Appliance der Phoenix Contact Cyber Security AG. Durch diesen Formfaktor lässt sich der mGuard pci² flexibel in jedes Gerät oder Maschine mit PCI- (mGuard pci²) oder PCI-Express-Bus (mGuard pcie²) integrieren. So können unternehmenskritische Rechner, Maschinen oder ganze Netze zuverlässig und sicher vor Angriffen geschützt werden.

Diese Packungsbeilage beinhaltet die Kurzbeschreibung zur Einrichtung Ihres mGuard pci² und enthält wichtige Hinweise zur Inbetriebnahme.

1. Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss der mGuard pci² richtig installiert, betrieben und gewartet werden. Bitte verwenden Sie den mGuard pci² ausschließlich auf die dafür vorgesehene Art und für geeignete Zwecke. Diese können im entsprechenden mGuard Handbuch nachgeschlagen werden. Das Benutzerhandbuch sowie weitere Produktinformationen finden Sie im Download-Bereich der PHOENIX CONTACT Cyber Security-Website unter http://www.phoenixcontact-cybersecurity.com/.

Schließen Sie die RJ45 Ethernet-Ports des mGuard pci² nur an passende Netzwerk-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen; diese dürfen nicht mit den RJ45-Anschlüssen des mGuard pci² verbunden werden.

2. Technische Grenzwerte

Das Produkt ist ausschließlich für die Verwendung innerhalb der in den Datenblättern angegebenen technischen Grenzwerte bestimmt.

Folgende Grenzwerte sind einzuhalten:

- Die Umgebungstemperaturgrenzen von 0 - +60° C (Betrieb) und -20 - +60° C (Lagerung/Transport) dürfen nicht unter- bzw. überschritten werden. HT Variante, ohne Akku [8]: 0 - +70° C (Betrieb) und -20 - +70° C (Lagerung/Transport).
- Versorgungsspannung 3,3V DC, max. 3,3W.
- Die Luftfeuchtigkeit darf nicht außerhalb des Bereichs von 5 – 95% liegen, Kondensatbildung muss vermieden werden.

Warnung:
Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann Funkstörungen verursachen. In diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

Pflichten des Betreibers
Der Betreiber muss grundsätzlich die in seinem Land geltenden nationalen Vorschriften bezüglich Betrieb, Funktionsprüfung, Reparatur und Wartung von elektronischen Geräten beachten.

Qualifikation des Personals
Die Installation, Inbetriebnahme und Wartung des Produkts darf nur durch ausgebildetes Fachpersonal erfolgen, das vom Anlagenbetreiber dazu autorisiert wurde. Das Fachpersonal muss diese Dokumentation gelesen und verstanden haben und die Anweisungen befolgen.

Sicherheitshinweise zum Transport
Die folgenden Hinweise sind zu beachten:

- Das Produkt darf während des Transports keiner Feuchtigkeit ausgesetzt werden. Das Produkt ist entsprechend zu verpacken.
- Das Produkt bitte so verpacken, dass es vor Erschütterungen beim Transport geschützt ist, z.B. durch eine luftgepolsterte Verpackung.

Das Produkt ist vor der Installation auf mögliche Beschädigungen zu überprüfen, die durch unsachgemäßen Transport entstanden sein könnten. Transportschäden müssen auf den Frachtpapieren festgehalten werden. Alle Schadensersatzansprüche sind unverzüglich und vor der Installation gegenüber dem Spediteur geltend zu machen.

3. Sicherheitshinweise zur elektrischen Installation

Der elektrische Anschluss darf nur von autorisiertem Fachpersonal gemäß den Elektroplänen vorgenommen werden. Bitte die Hinweise zum elektrischen Anschluss in der Anleitung beachten, ansonsten kann die elektrische Schutzart beeinträchtigt werden.
Die sichere Trennung von berührungsgefährlichen Stromkreisen ist nur gewährleistet, wenn die angeschlossenen Geräte die Anforderungen der VDE 0106 T101 (Sichere Trennung) erfüllen. Für die sichere Trennung sind die Zuleitungen getrennt von berührungsgefährlichen Stromkreisen zu führen oder zusätzlich zu isolieren.

4. Gewährleistungsbestimmungen

Eine nicht bestimmungsgemäße Verwendung, ein Nichtbeachten dieser Dokumentation, der Einsatz von nicht ausreichend qualifiziertem Personal sowie eigenmächtige Veränderungen schließen die Haftung des Herstellers für daraus resultierende Schäden aus. Hierbei erlischt die Gewährleistung des Herstellers.

5. Haftungsbeschränkung

Diese Kurzbeschreibung soll die hierin beschriebenen Inhalte und Prozesse wiedergeben und wird regelmäßig überprüft. Da es jedoch nicht möglich ist sicherzustellen, dass die Inhalte und Prozesse in jeder Hinsicht richtig dargestellt sind, ist die Haftung für die hierin getroffenen Aussagen oder Einschätzungen ausgeschlossen. Bitte beachten Sie auch, dass technische Daten jederzeit geändert werden können.

6. Übersicht

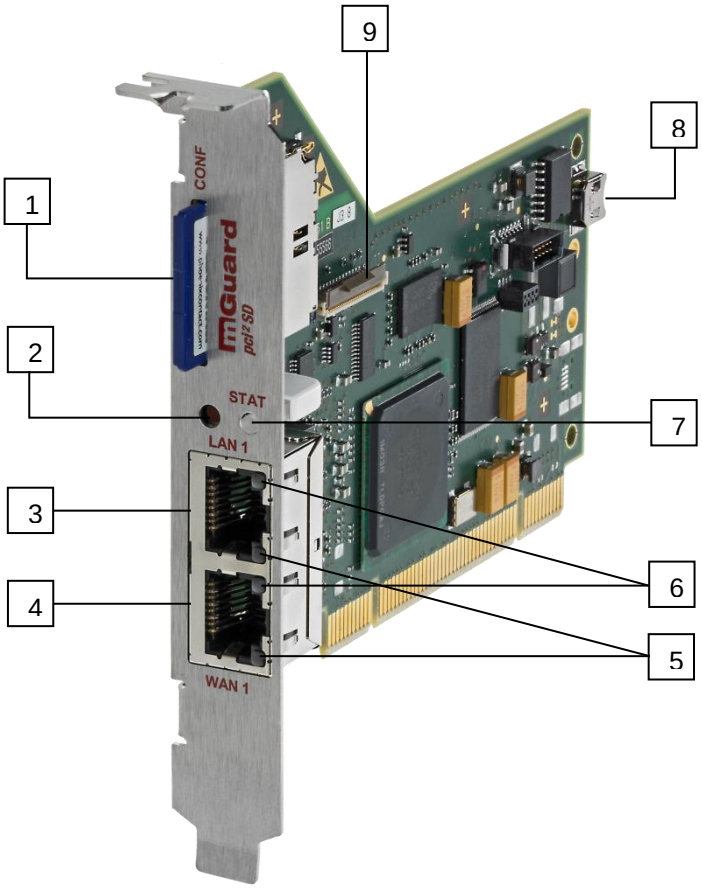


Abbildung 1: mGuard pci² | Anschlussbelegungen Frontseite

1 SD-Karten Slot (Konfigurationsspeicher)

2 Reset-Schalter

3 RJ45 Buchse **(LAN 1)** der internen Netzwerkschnittstelle für den Anschluss an das interne Netzwerk; benutzen Sie ein UTP-Kabel (CAT 5); das Kabel ist nicht im Lieferumfang enthalten

4 RJ45 Buchse **(WAN 1)** der externen Netzwerkschnittstelle für den Anschluss an das externe Netzwerk/Internet; benutzen Sie ein UTP-Kabel (CAT 5); das Kabel ist nicht im Lieferumfang enthalten

5	LAN/WAN Ethernet-Buchse:	Duplex/Half Duplex	(grün an/aus)
6	LAN/WAN Ethernet-Buchse:	Speed/Link/Daten	(gelb/grün an/aus/blinkend)

Die ersten drei LEDs [5], [6] der LAN/WAN Ethernet-Buchsen bilden eine Lauflichtsequenz während der Recovery- und Flashing-Prozedur.

7 STAT LED: Diagnose & Status Indikator

Rot/Grün blinkend:	Bootprozess	Nach Anlegen der Betriebsspannung. Die LED wechselt nach einigen Sekunden in den Heartbeat-Modus.
Grün blinkend:	Heartbeat	Der mGuard ist korrekt angeschlossen und funktionsfähig.
Rot blinkend:	Systemfehler	Starten Sie den mGuard neu. Drücken Sie hierzu kurz den Reset-Schalter für 1,5 Sekunden. Alternativ schalten Sie das System aus, so dass der mGuard von der Spannungsversorgung getrennt wird, und schalten das System wieder ein. Sollte der Fehler erneut auftreten, so führen Sie bitte die mGuard Recovery-Prozedur wie im mGuard Benutzerhandbuch beschrieben, durch.

8 Akku (austauschbar)

9 Erweiterungsanschluss (LEDs, Reset-Schalter, SD-Karte)

7. Inbetriebnahme

Verfahren Sie wie im Handbuch Ihres Systems beschrieben, um den mGuard pci² in einen freien PCI (mGuard pci²) oder PCI-Express (mGuard pcie²) Steckplatz einzubauen. Vermeiden Sie dabei Schäden an den Baugruppen durch elektrostatische Aufladungen (ESD Vorschriften beachten).

Der mGuard pci² kann auf drei unterschiedliche Vorgehensweisen in Betrieb genommen werden:

7.1 Gerät im ´Stealth-Modus´ in Betrieb nehmen (Standard)

Den mGuard pci² wie folgt in eine bestehende Netzwerkverbindung zwischenschalten:

- Verbinden Sie die interne Netzwerkschnittstelle (LAN 1) des mGuard pci² mit einem geeigneten UTP-Kabel (CAT5) mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners bzw. einem validen Netzwerk-Anschluss des internen Netzwerks. Das Kabel ist nicht im Lieferumfang enthalten.

- Verbinden Sie die externe Netzwerkschnittstelle (WAN 1) des mGuard pci² mit einem geeigneten UTP-Kabel (CAT5) mit dem externen Netzwerk bzw. Internet. Das Kabel ist nicht im Lieferumfang enthalten.

- Schalten Sie das System ein. Die mGuard pci² Status-Anzeige STAT leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.

- Der mGuard bootet die Firmware. Die Status-Anzeige STAT blinkt währenddessen grün.

- Der mGuard ist betriebsbereit, sobald die Link-LEDs der Ethernet-Buchsen (LAN1 / WAN 1) leuchten. Zusätzlich blinkt die Status-Anzeige STAT grün im Heartbeat.

Hinweis: Eine fehlende Konnektivität des internen oder externen Netzwerks wird durch die jeweils **nicht** leuchtende Link-LED in den Ethernet-Buchsen gemeldet.
Sollte keine der Status- und Diagnose-Anzeigen leuchten, so fehlt die korrekte Versorgungsspannung.

Über einen lokal angeschlossenen Rechner (z.B. der Schützling) mit einem HTTPS-fähigen Web-Browser (z. B. Mozilla Firefox, Google Chrome, Microsoft Internet Explorer) kann der mGuard pci² über das interne Netzwerk nun sicher konfiguriert werden. Das verwendete HTTPS-Protokoll wird zur Verschlüsselung und zur Authentifizierung der Kommunikation zwischen dem mGuard pci² und dem Browser verwendet.

Im Browser bitte die folgende Adresse eingeben: https://1.1.1.1/

7.1.1 Konfiguration des mGuards

Die Verbindung zum mGuard pci² wird hergestellt. Der Sicherheitshinweis wegen eines angeblich ungültigen/nicht vertrauenswürdigen Zertifikats wird angezeigt. Diese Meldung resultiert aus der Verwendung eines mGuard-eigenen Zertifikats, welches dem Browser noch unbekannt, jedoch zur Verschlüsselung der Kommunikation zwingend notwendig ist.

Quittieren Sie den Hinweis mit:
´Dieses Zertifikat immer/temporär akzeptieren´ (Firefox), ´Laden dieser Website fortsetzen´ (Internet Explorer), ´Trotzdem Fortfahren´ (Chrome).

Die Anmeldemaske des mGuard pci² erscheint.

Abbildung 2: mGuard pci² | Anmeldemaske

Wählen Sie die Zugangsart ´Administration´ und geben Sie bitte zum erstmaligen Anmelden den folgenden Default-Benutzernamen und -Passwort ein (Groß- / Kleinschreibung beachten):

Benutzername:	**admin**
Passwort:	**mGuard**
Zugangsart:	**Administration**

Nach erfolgreicher Anmeldung wird die integrierte mGuard Konfigurations- und Administrationsoberfläche angezeigt. Nun können Sie mit der Konfiguration des mGuard pci² beginnen.

7.2 Gerät über temporäre Management IP-Adresse in Betrieb nehmen

Wenn im Erstinbetriebnahme-Modus die externe Netzwerkschnittstelle (WAN 1) des mGuard pci² nicht an ein funktionierendes Netzwerk angeschlossen wird, so ist das Gerät unter der Adresse https://1.1.1.1/ (siehe „Gerät im ´Stealth-Modus´ in Betrieb nehmen“) **nicht** erreichbar.

Der mGuard pci² wird in diesem Fall automatisch über die Management IP-Adresse 192.168.1.1/24 sowohl über die interne (LAN 1) als auch externe (WAN 1) Netzwerkschnittstelle erreichbar. Ein Adressenkonflikt an der externen Netzwerkschnittstelle (WAN 1) ist nicht möglich, solange diese nicht an ein funktionierendes Netzwerk angeschlossen wird. Diese Management IP-Adresse ist normalerweise nicht persistent.

Wird nach dem Hochfahren des mGuard pci² jedoch die externe Netzwerkschnittstelle (WAN 1) nachträglich verbunden, bleibt die Management IP-Adresse bestehen und ein Adressenkonflikt mit bereits bestehenden Adressen im externen Netzwerk wäre möglich.

- Verbinden Sie die interne Netzwerkschnittstelle (LAN 1) des mGuard pci² mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners bzw. einem validen Netzwerk-Anschluss des internen Netzwerks.
- Trennen Sie die externe Netzwerkschnittstelle (WAN 1) des mGuard pci² vom externen Netzwerk (WAN).
- Schalten Sie das System ein. Die mGuard pci² Status-Anzeige STAT leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.
- Der mGuard bootet die Firmware. Die Status-Anzeige STAT blinkt grün.
- Der mGuard ist betriebsbereit, sobald die Link-LED der LAN 1 Ethernet-Buchse leuchtet. Die Link-LED der WAN 1 Ethernet-Buchse bleibt dunkel. Zusätzlich blinkt die Status-Anzeige STAT grün im Heartbeat.

Hinweis: Sollte keine der Status- und Diagnose-Anzeigen leuchten, so fehlt die korrekte Versorgungsspannung.

7.2.1 Anpassen des Konfigurationsrechners

Um den mGuard pci² für die Konfiguration erreichen zu können, muss der Konfigurationsrechner an die Management IP-Adresse des mGuard pci² angepasst werden (Beispiel Microsoft Windows XP):

Im Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)“ der betreffenden Netzwerkschnittstelle des Konfigurationsrechners die Einstellungen wie folgt setzen:

- IP-Adresse: 192.168.1.10
- Subnetzmaske: 255.255.255.0
- Standardgateway: 192.168.1.2

- Im Web-Browser die folgende Adresse eingeben: https://192.168.1.1/
- Konfigurieren Sie den mGuard wie im Abschnitt 7.1.1 beschrieben.

7.3 Gerät per BootP in Betrieb nehmen

Der mGuard pci² startet im Erstinbetriebnahme-Modus immer zusätzlich einen BootP-Client an der internen Netzwerkschnittstelle (LAN 1). Der BootP-Client ist kompatibel zu den BootP-Servern ´IPassign´ von Phoenix Contact sowie ´DHCPD´ unter Linux. Das englische Windows-Programm ´IPassign´ kann unter den folgenden Adressen kostenlos heruntergeladen werden:

- http://www.phoenixcontact-cybersecurity.com/ > Downloads > Software
- http://www.phoenixcontact.com/automation/32119_30373.htm

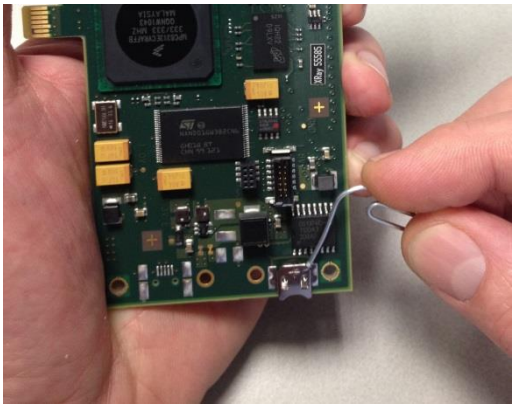
Erreicht ein nicht konfigurierter mGuard pci² nach dem Hochfahren einen BootP-Server, wird über das BootP-Protokoll dem mGuard pci² eine IP-Adresse (z.B. 192.168.10.4), eine Netzwerk-Maske (z.B. 255.255.255.0) und optional ein Standard-Gateway der internen Netzwerkschnittstelle zugewiesen. Diese Parameter werden persistent im Gerät gespeichert, welches dann ab sofort darunter erreichbar ist.

- Im Web-Browser die per BootP zugewiesene Adresse eingeben: z.B. https://192.168.10.4/
  Konfigurieren Sie den mGuard wie im Abschnitt 7.1.1 beschrieben.

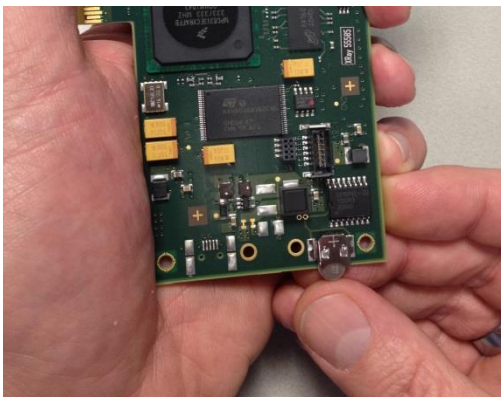
7.4 Auswechseln der Batterie

Der mGuard pci^2 , außer der HT Variante, ist mit einem Akku ausgestattet. Bei Bedarf kann dieser gewechselt werden.
Verwenden Sie nur Akkus des Typs Panasonic ML621.

(1) Benutzen Sie einen spitzen und langen Gegenstand, Beispielsweise eine aufgebogene Büroklammer, um den Akku aus seiner Halterung zu entfernen.



(2) Schieben Sie den neuen Akku in die Halterung.
Achtung: Achten Sie unbedingt auf die Polarität!



8 Fehlerbehebung

8.1 Keine Verbindung zum mGuard

Falls keine Verbindung zum mGuard pci² hergestellt werden kann, gehen Sie bitte wie folgt vor:

- Kontrollieren Sie alle Stecker und Anschlüsse auf korrekten Sitz und Funktion mit Hilfe der Diagnose- und Status-Anzeigen.
- Entfernen Sie den mGuard pci² aus dem System und installieren Sie den mGuard pci² in einem anderen System.
- Tauschen Sie die Netzwerkkabel für das interne und externe Netzwerk (LAN 1 / WAN 1) aus.
- Benutzen Sie wenn möglich andere Netzwerkanschlüsse am internen bzw. externen Netzwerk.
- Deaktivieren Sie für die Dauer der Konfiguration eine mögliche bestehende Software-Firewall auf ihrem Rechner (z.B. Windows 7, Windows Vista).
- Deaktivieren Sie für die Dauer der Konfiguration eine mögliche bestehende Antivirus-Software auf ihrem Rechner.
- Benutzen Sie einen anderen Browser und achten Sie auf die zwingende Verwendung der Syntax ´https://´ statt ´http://´.
- Benutzen Sie zum Konfigurieren vorübergehend einen anderen Rechner.

8.2 Keine Verbindung zum mGuard via ´https://1.1.1.1 (Stealth-Modus)

Bei einem fehlenden oder fehlerhaften Standardgateway des Konfigurationsrechners kann über die Adresse https://1.1.1.1/ nicht auf den mGuard pci² zugegriffen werden. In diesem Fall ist das Standardgateway des Konfigurationsrechners wie folgt zu initialisieren (Beispiel für Microsoft Windows XP):

Im Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)“ der betreffenden Netzwerkschnittstelle des Konfigurationsrechners die Adresse des Standardgateways ermitteln oder, falls nicht vorhanden, wie folgt setzen:

- IP-Adresse: 192.168.1.1
- Subnetzmaske: 255.255.255.0
- Standardgateway: 192.168.1.2

Anschließend in der Eingabeaufforderung (Menü: Start, Alle Programme, Zubehör, Eingabe-aufforderung) folgendes Kommando eingeben (sofern 192.168.1.2 die ermittelte oder festgelegte IP-Adresse des Standardgateways ist):

arp -s 192.168.1.2 00-aa-aa-aa-aa-aa

Über die interne Netzwerkschnittstelle kann jetzt auf den mGuard pci² unter der Adresse https://1.1.1.1/ zugegriffen werden.

Nach der Konfiguration des mGuard pci² stellen Sie das Standardgateway wieder zurück. Dazu entweder den Konfigurationsrechner neu starten oder in der Eingabeaufforderung folgendes Kommando eingeben:

arp -d

Je nachdem, wie Sie den mGuard pci² konfigurieren, müssen Sie gegebenenfalls anschließend die Netzwerkschnittstelle des lokal angeschlossenen Rechners bzw. Netzes entsprechend anpassen.

Package slip // mGuard pci² product family

mGuard pci² SD	Order number:	HW-102061
mGuard pci² SD VPN	Order number:	BD-111040
mGuard pci² SD HT VPN	Order number:	BD-111070
mGuard pcie² SD	Order number:	HW-102071
mGuard pcie² SD VPN	Order number:	BD-111060

EN Installation notes for electrical personnel

Thank you for putting your trust in the mGuard product range. The mGuard pci² is a compact, PCI compatible firewall/router/VPN appliance from Phoenix Contact Cyber Security AG. Its design factor enables the mGuard pci² card to be flexibly integrated into every device or machine with a PCI- (mGuard pci²) or PCI-Express (mGuard pcie²) bus. Thus it is an ideal solution to protect critical systems, machines or complete networks against attacks.

This package slip contains a brief description for setting up your mGuard pci² and contains important instructions for startup.

1. Safety notes

To ensure correct operation and the safety of the environment and of personnel, the mGuard pci² must be installed, operated, and maintained correctly. Please use the mGuard pci² for its intended purpose as suited. These can be looked up in the relevant mGuard manual. The user manual as well as additional product information can be found in the download area of the PHOENIX CONTACT Cyber Security website at http://www.phoenixcontact-cybersecurity.com/.

Connect the RJ45 Ethernet ports plug of the mGuard pci² to LAN installations only. Some telecommunications connections also use RJ45 sockets and these must not be connected to the RJ45 connections of the mGuard pci².

2. Technical limit values

The product is intended for use only within the technical limit values specified in the data sheets.

The following limit values must be observed:

- Do not go below or exceed the ambient temperature range of 0 - +60° C (operating) and -20 - +60° C (storage/transport). HT model without battery [8]: 0 - +70° C (operating) and -20 - +70° C (storage/transport).
- Supply voltage 3,3V DC, max. 3,3W.
- An air humidity range of 5 - 95% must not be exceeded and formation of condensation must be avoided.

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

Responsibility of the operator
The operator must comply with all current national regulations with respect to operation, function testing, repairs and maintenance of electronic devices.

Staff qualification
The installation, startup and maintenance of the product may only be performed by qualified specialist staff. Specialist staff must read and understand this documentation and comply with instructions.

Safety instructions for transporting
The following instructions must be observed:
- do not subject the product to humidity during transit. Pack the product accordingly.
- pack the product in such a way that it is protected against shock during transit, e.g. in padded packaging.

Before installing, check the product for possible damage caused by inappropriate transport. Transport damage must be recorded in the shipping documents. All claims for damage must be made to the shipping company immediately and prior to installation.

3. Safety instructions for the electrical installation

Electrical connection may only be performed according to circuit diagrams by authorized specialist staff. Observe the instructions on the electrical connection in order not to adversely affect the degree of electrical protection. Safe isolation of live circuits is only guaranteed if connected devices fulfill requirements specified by VDE 0106 T.101 (safe isolation). Additionally isolate or lay supply lines to live circuits separately.

4. Warranty conditions

The manufacturer is not liable for damages resulting from failure to use for not intended purpose, failure to observe this documentation, failure to deploy adequately qualified staff as well as unauthorized modification. The warranty conditions of the manufacturer expire.

5. Limitations on liability

This brief description is intended to explain the content and processes described and undergoes regular checking. Because it is not possible to guarantee that the content and processes are correct in all respects, liability is excluded for all statements or estimates within. Please also be aware that technical data can be changed at any time.

6. Overview

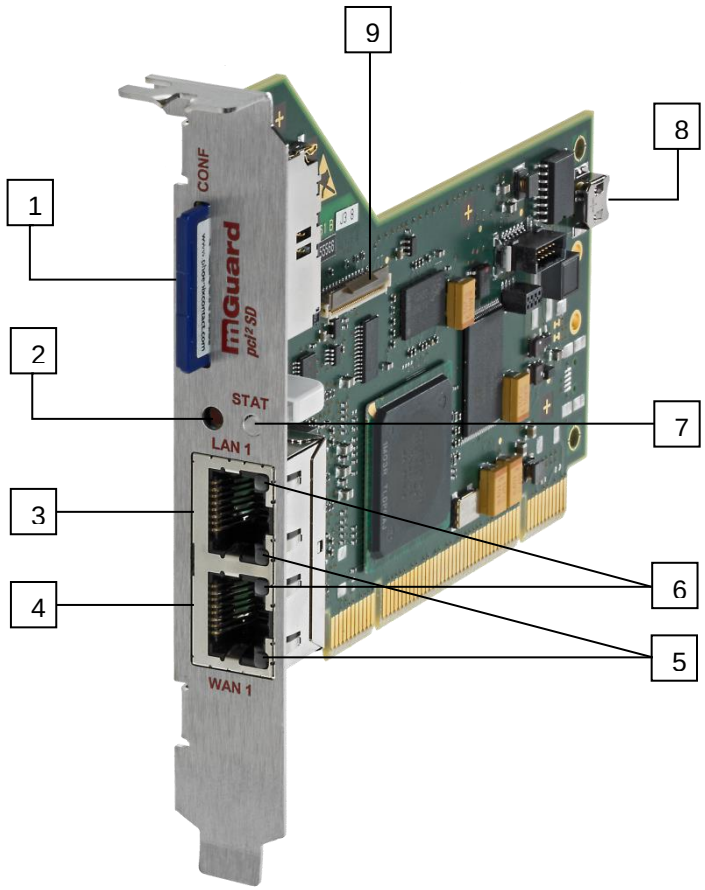


Figure 1: mGuard pci² | assignment front panel

1 SD-Card slot (configuration memory)

2 Reset switch

3 RJ45 socket **(LAN 1)** of the internal network interface for the connection to the **internal network**; a suitable UTP cable (CAT 5) is needed for that, which is not included in the scope of delivery

4 RJ45 socket **(WAN 1)** of the external network interface for the connection to the **external network/Internet**; a suitable UTP cable (CAT 5) is needed for that, which is not included in the scope of delivery

5 LAN/WAN Ethernet socket: duplex/half duplex (green on/off)

6 LAN/WAN Ethernet socket: speed/link/data (yellow/green on/off/flashing)

The first three LEDs [5], [6] of the LAN/WAN Ethernet sockets form a light sequence while recovery and flashing procedure.

7 STAT LED: Diagnostics & status indicators

Red/Green flashing:	Boot process	After connecting the device to the power supply. The LED switches to heartbeat mode after a few seconds.
Green Flashing:	Heartbeat	The device is correctly connected and functioning.
Red Flashing:	System error	Reboot the system. Press the Rescue button briefly (1.5 seconds). Alternatively, disconnect the device from its power supply briefly, then reconnect it. If the error continues to occur, start the recovery procedure as described in the mGuard User Manual.

8 Battery (exchangeable)

9 Extension port (LEDs, reset button, SD card)

7. Installation

In order to install the mGuard pci² board into a free PCI (mGuard pci²) or PCI Express (mGuard pcie²) slot of your system carefully follow all of the corresponding instructions in the appropriate chapter in your system‘s manual. Please also make sure to observe all precautions for the handling of electrostatic devices.

The mGuard pci² can be set up in three different ways:

7.1 Operation in ´stealth mode´ (default)

Insert the mGuard pci² into an existing network connection as follows

- Connect the network interface LAN 1 of the mGuard pci² with a suitable UTP cable (CAT5) to the corresponding Ethernet network card of the configuration computer or a valid network connector of the internal network.
- Connect the network interface WAN 1 of the mGuard pci² with a suitable UTP cable (CAT5) to the external network/Internet.
- Switch the system on. The status indicator STAT lights up green when the supply voltage has been connected properly.
- The mGuard boots the firmware. The status indicator STAT flashes green.
- The mGuard is ready for operation as soon as the link LEDs of the Ethernet socket light up.
- Additionally, the status indicator STAT flashes green at heartbeat.

Hint: Status displays within the corresponding Ethernet socket that do not light up indicate a failure to connect to the internal or external network.
If the no status or diagnostics display light up, this is due to incorrect power supply.

The mGuard pci² can now be safely configured via a locally connected computer in the internal network using a HTTPS-capable web browser (e.g., Mozilla Firefox, Google Chrome, Microsoft Internet Explorer). The HTTPS protocol is used for encryption and authentication of the communication between the mGuard pci² and the browser.

Enter the following address in the browser: https://1.1.1.1/

7.1.1 Configuring the mGuard

A connection to mGuard pci² is established. A security message indicating a possible invalid/not trusted certificate is displayed. This message results from the use of an mGuard certificate that is not yet known to the browser but necessary for encryption of the communication.

Confirm this message with: ´Accept this certificate always/temporarily´ (Firefox), ´Continue loading this website´ (Internet Explorer), ´Continue anyway´ (Chrome).

The Login form of mGuard pci² is displayed. (Fig. 2).

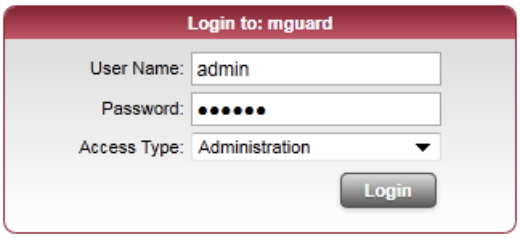


Figure 2: mGuard pci² | login form

Select ´Administration´ as access type and enter the default user name and password when using for the first time (case sensitive):

User Name: **admin**
Password: **mGuard**
Access Type: **Administration**

After successful login, the integrated mGuard configuration and administration interface is displayed. Now you can begin with the configuration of your mGuard pci².

7.2 Putting mGuard into operation without a functioning network

If the external mGuard network interface WAN 1 is not connected to a functioning network during the initial startup, the device is not accessible under the address https://1.1.1.1/.

In this case, the mGuard is accessible automatically by the management IP address 192.168.1.1/24. An address conflict with the external network interface is not possible as long as a functioning network is not connected. This management IP address is normally not saved.

You have started up the mGuard without a functioning network being connected to the network interface (WAN 1). If you connect the mGuard now retroactively to an external network (WAN 1), the management IP address is maintained. There is a possibility thereby that there may be an address conflict with already existing addresses in the external network.

Proceed as follows to reach the mGuard via the management IP address:

- Connect the network interface LAN 1 of the mGuard with a suitable UTP cable (CAT5) to the corresponding Ethernet network card of the configuration computer or a valid network connector of the internal network.
- Leave the external network interface (WAN 1) disconnected from the external network (WAN).
- Switch the system on. The status indicator STAT lights up green when the supply voltage has been connected properly.
- The mGuard boots the firmware. The status indicator STAT flashes green.

- The mGuard is ready for operation as soon as the link LED of the LAN 1 Ethernet socket light up. The LED of the WAN 1 socket remains off.

- Additionally, the status indicator STAT flashes green at heartbeat.

Hint: If none of the status or diagnostics LED light up, this is due to incorrect connection voltage.

7.2.1 Adjusting the configuration computer

This is how you adjust the configuration computer to the management IP address of the mGuard pci2. The following explanation applies to Microsoft Windows XP:

- Open the Control Panel on the configuration computer and double-click the Network Connections.
- Select the respective network interface and click on “Properties” in the context menu.
- Select the “Internet Protocol (TCP/IP)” and click on the “Properties” button.
- Enter the following:
  - IP address: 192.168.1.10
  - Subnet mask: 255.255.255.0
  - Default gateway: 192.168.1.2

- Enter the following address into the web browser: https://192.168.1.1/
- Configure the mGuard as described in section 7.1.1.

7.3 Starting up the mGuard using BootP

You can also start up the mGuard using the BootP protocol. In initial startup mode, the mGuard additionally starts a BootP client at the internal network interface LAN 1. This BootP client is compatible to the BootP servers “IPassign” from Phoenix Contact as well as “DHCPD” under Linux.

You can download an English Windows program “IPassign“ at the following addresses at no cost:

- http://www.innominate.com/ > Downloads > Software
- http://www.phoenixcontact.com/automation/32119_30373.htm

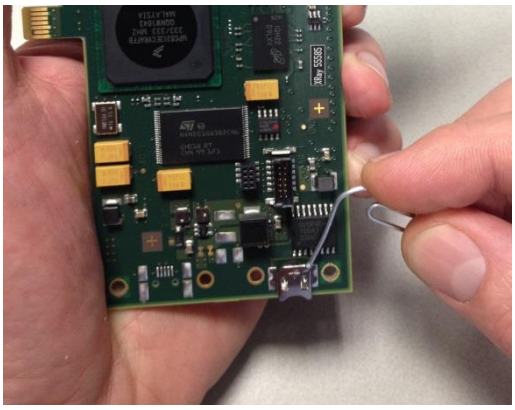
If a non-configured mGuard reaches a BootP server after starting up, then addresses are assigned to the mGuard. The BootP protocol assigns the mGuard an IP address (e.g. 192.168.10.4), a subnet mask (e.g. 255.255.255.0) and optionally a default gateway of the internal network interface. These parameters are saved in the device, which is accessible immediately then by these parameters.

- In the web browser however, enter the address (e.g. https://192.168.10.4) that was assigned to the mGuard by BootP.
- Configure the mGuard as described in section 7.1.1.

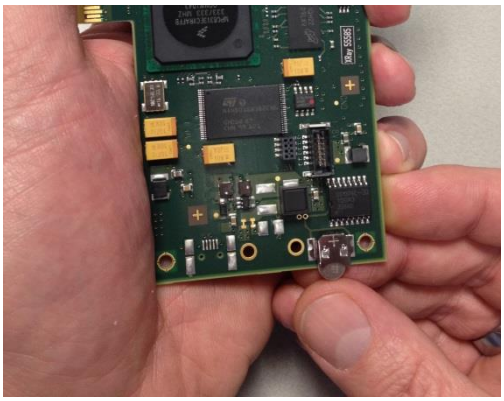
7.5 Replacing the Battery

The mGuard pci² is, except of the HT model, equipped with a rechargeable battery. If necessary, this battery can be replaced.
Replace cell with lithium/manganese cell by PANASONIC CORPORATION, type ML621 only. Use of another cell may present a risk of fire or explosion.

(1) Use a sharp and long object, for example a straightened paper clip, to remove the battery from its holder.



(2) Push the new battery into the holder. Caution: Observe the polarity!



Dispose of used cell promptly. Keep away from children. Do not disassemble and do not dispose of in fire.

Caution:
The cell used in this device may present a risk of fire or chemical burn hazard if mistreated. Do not disassemble, expose to heat above 100°C (212°F) or incinerate. Replace cell with Lithium/Manganese Cell by PANASONIC CORPORATION, type ML621 only. Use of another cell may present a risk of fire or explosion.

8 Troubleshooting

8.1 No connection to mGuard

If no connection to the mGuard can be established, proceed as follows:

- Check that all plugs and connections are securely fixed. Check the status indicators.
- Remove the mGuard pci² from the system and install the mGuard pci² into a different system.
- Replace the network cables of the external (WAN 1) and internal (LAN 1) networks.
- Use other network connections of the internal or external network.
- Deactivate a possible existing software firewall on your computer during configuration (e.g. Windows 7, Windows Vista).
- Deactivate existing antivirus software on your computer during configuration.
- Use a different browser and make sure you enter ´https://´ instead of ´http://´.
- Temporarily use a different computer for configuration.

8.2 No connection to the mGuard via ´https://1.1.1.1´ (stealth mode)

This section applies only for mGuard pci2 in stealth mode.

If you cannot access the mGuard via the https://1.1.1.1/ address, the cause may be a missing or faulty default gateway of the configuration computer. In this case, initialize the default gateway of the configuration computer as follows. The following explanation applies to Windows XP:

- Open the Control Panel on the configuration computer and double-click the Network Connections.
- Select the respective network interface and click on “Properties” in the context menu.
- Select the “Internet Protocol (TCP/IP)” and click on the “Properties” button.
- Read out the address. If none is available, enter the following:
    - IP address: 192.168.1.10
    - Subnet mask: 255.255.255.0
    - Default gateway: 192.168.1.2

Open the prompt (Start menu “All Programs/Accessories/DOS prompt”). The following entry depends on the default gateway. If, for example, 192.168.1.2 is the IP address of the default gateway, enter the following command:

arp -s 192.168.1.2 00-aa-aa-aa-aa-aa

You can now access the mGuard at the address https://1.1.1.1/.

After configuring the mGuard, reset the default gateway. Enter the following command into the input prompt for that:

arp –d

As an alternative, you can restart the configuration computer. 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.