Installation und Inbetriebnahme der mGuard-Hardware

Anwenderhandbuch

PHOENIX CONTACT
INSPIRING INNOVATIONS

Anwenderhandbuch
Installation und Inbetriebnahme der mGuard-Hardware

2022-11-08

Bezeichnung: UM DE MGUARD DEVICES

Revision: 09

Artikel-Nr.: —

Dieses Handbuch ist gültig für die folgenden Geräten der mGuard-Familie:

- FL MGUARD RS4000
- FL MGUARD RS2000
- FL MGUARD RS4004
- FL MGUARD RS2005
- TC MGUARD RS4000 3G
- TC MGUARD RS2000 3G
- TC MGUARD RS4000 4G (inkl. US-Varianten VZW und ATT)
- TC MGUARD RS2000 4G (inkl. US-Varianten VZW und ATT)
- FL MGUARD RS2000 TX/TX-B
- FL MGUARD RS4000 TX/TX-P
- FL MGUARD RS4000 TX/TX VPN-M
- FL MGUARD GT/GT
- FL MGUARD PCI(E)4000
- FL MGUARD SMART2
- FL MGUARD DELTA TX/TX
- FL MGUARD CENTERPORT

Bitte beachten Sie folgende Hinweise

Zielgruppe des Handbuchs

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen, die mit den geltenden Normen und sonstigen Vorschriften zur Elektrotechnik und insbesondere mit den einschlägigen Sicherheitskonzepten vertraut sind.

Erklärungen zu den verwendeten Symbolen und Signalwörtern

Dieses Symbol kennzeichnet Gefahren, die zu Personenschäden führen können. Beachten Sie alle Hinweise, die mit diesem Hinweis gekennzeichnet sind, um mögliche Personenschäden zu vermeiden.

Es gibt drei verschiedene Gruppen von Personenschäden, die mit einem Signalwort gekennzeichnet sind.

GEFAHR Hinweis auf eine gefährliche Situation, die – wenn sie nicht vermieden wird – einen Personenschaden bis hin zum Tod zur Folge hat.

WARNUNG Hinweis auf eine gefährliche Situation, die – wenn sie nicht vermieden wird – einen Personenschaden bis hin zum Tod zur Folge haben kann.

VORSICHT Hinweis auf eine gefährliche Situation, die – wenn sie nicht vermieden wird – eine Verletzung zur Folge haben kann.

Dieses Symbol mit dem Signalwort **ACHTUNG** und der dazugehörige Text warnen vor Handlungen, die einen Schaden oder eine Fehlfunktion des Gerätes, der Geräteumgebung oder der Hard-/Software zur Folge haben können.

Dieses Symbol und der dazugehörige Text vermitteln zusätzliche Informationen oder verweisen auf weiterführende Informationsquellen.

So erreichen Sie uns

Internet

Aktuelle Informationen zu Produkten von Phoenix Contact und zu unseren Allgemeinen Geschäftsbedingungen finden Sie im Internet unter:
phoenixcontact.com.

Stellen Sie sicher, dass Sie immer mit der aktuellen Dokumentation arbeiten.
Diese steht unter der folgenden Adresse zum Download bereit:
phoenixcontact.net/products.

Ländervertretungen

Bei Problemen, die Sie mit Hilfe dieser Dokumentation nicht lösen können, wenden Sie sich bitte an Ihre jeweilige Ländervertretung.
Die Adresse erfahren Sie unter phoenixcontact.com.

Herausgeber

PHOENIX CONTACT GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg
DEUTSCHLAND

Wenn Sie Anregungen und Verbesserungsvorschläge zu Inhalt und Gestaltung unseres Handbuchs haben, würden wir uns freuen, wenn Sie uns Ihre Vorschläge zusenden an:
tecdoc@phoenixcontact.com

Allgemeine Nutzungsbedingungen für Technische Dokumentation

Phoenix Contact behält sich das Recht vor, die technische Dokumentation und die in den technischen Dokumentationen beschriebenen Produkte jederzeit ohne Vorankündigung zu ändern, zu korrigieren und/oder zu verbessern, soweit dies dem Anwender zumutbar ist. Dies gilt ebenfalls für Änderungen, die dem technischen Fortschritt dienen.

Der Erhalt von technischer Dokumentation (insbesondere von Benutzerdokumentation) begründet keine weitergehende Informationspflicht von Phoenix Contact über etwaige Änderungen der Produkte und/oder technischer Dokumentation. Sie sind dafür eigenverantwortlich, die Eignung und den Einsatzzweck der Produkte in der konkreten Anwendung, insbesondere im Hinblick auf die Befolgung der geltenden Normen und Gesetze, zu überprüfen. Sämtliche der technischen Dokumentation zu entnehmenden Informationen werden ohne jegliche ausdrückliche, konkludente oder stillschweigende Garantie erteilt.

Im Übrigen gelten ausschließlich die Regelungen der jeweils aktuellen Allgemeinen Geschäftsbedingungen von Phoenix Contact, insbesondere für eine etwaige Gewährleistungshaftung.

Phoenix Contact behält sich das Recht vor, für die hier verwendeten Produktkennzeichnungen von Phoenix Contact-Produkten eigene Schutzrechte anzumelden. Die Anmeldung von Schutzrechten hierauf durch Dritte ist verboten.

Andere Produktkennzeichnungen können gesetzlich geschützt sein, auch wenn sie nicht als solche markiert sind.

FCC Note

The FCC Statement applies to the following devices:

Class A: FL MGUARD RS4000, FL MGUARD RS2000, FL MGUARD RS4004,
FL MGUARD RS2005, FL MGUARD SMART2, FL MGUARD PCI4000,
FL MGUARD DELTA TX/TX, FL MGUARD GT/GT, FL MGUARD RS2000 TX/TX-B,
FL MGUARD RS4000 TX/TX-P, FL MGUARD RS4000 TX/TX VPN-M
Class B: TC MGUARD RS4000 3G, TC MGUARD RS2000 3G, FL MGUARD RS4000 4G,
FL MGUARD ES2000 4G, FL MGUARD CENTERPORT

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.

FCC Statement

Class A	Class B
This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant 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.

Inhaltsverzeichnis

1 Zu Ihrer Sicherheit 11

1.1 Kennzeichnung der Warnhinweise 11
1.2 Über dieses Handbuch 11
1.3 Qualifikation der Benutzer 11
1.4 Bestimmungsgemäße Verwendung 12
1.5 Veränderung des Produkts 12
1.6 Sicherheitshinweise 12
1.7 IT-Sicherheit 14
1.8 Aktuelle Sicherheitshinweise zu Ihrem Produkt 16
1.9 Support 16

2 FL MGUARD RS4000/RS2000 17

2.1 Bedienelemente und Anzeigen 18
2.2 Inbetriebnahme 20
2.3 FL MGUARD RS4000/RS2000 installieren 21
2.4 Konfiguration vorbereiten 27
2.5 Konfiguration im Stealth-Modus 28
2.6 Lokale Konfigurationsverbindung herstellen 31
2.7 Fernkonfiguration 33
2.8 Serielle Schnittstelle 33
2.9 Neustart, Recovery-Prozedur und Flashen der Firmware 34
2.10 Technische Daten 39

3 FL MGUARD RS4004/RS2005 41

3.1 Bedienelemente und Anzeigen 42
3.2 Inbetriebnahme 44
3.3 FL MGUARD RS4004/RS2005 installieren 45
3.4 Konfiguration vorbereiten 50
3.5 Konfiguration im Router-Modus 50
3.6 Lokale Konfigurationsverbindung herstellen 51
3.7 Fernkonfiguration 53
3.8 Serielle Schnittstelle 53
3.9 Neustart, Recovery-Prozedur und Flashen der Firmware 54
3.10 Technische Daten 59

4 TC MGUARD RS4000/RS2000 3G 61

4.1 Bedienelemente und Anzeigen 62
4.2 Inbetriebnahme 64
4.3 TC MGUARD RS4000/RS2000 3G installieren 65

4.4 Konfiguration vorbereiten ... 72
4.5 Konfiguration im Router-Modus ... 72
4.6 Lokale Konfigurationsverbindung herstellen ... 73
4.7 Fernkonfiguration ... 75
4.8 Serielle Schnittstelle ... 75
4.9 Neustart, Recovery-Prozedur und Flashen der Firmware ... 76
4.10 Technische Daten ... 81

5 TC MGUARD RS4000/RS2000 4G ... 83
5.1 Bedienelemente und Anzeigen ... 85
5.2 Inbetriebnahme ... 87
5.3 TC MGUARD RS4000/RS2000 4G installieren ... 88
5.4 Konfiguration vorbereiten ... 96
5.5 Konfiguration im Router-Modus ... 96
5.6 Lokale Konfigurationsverbindung herstellen ... 97
5.7 Fernkonfiguration ... 99
5.8 Serielle Schnittstelle ... 99
5.9 Neustart, Recovery-Prozedur und Flashen der Firmware ... 100
5.10 Technische Daten ... 104

6 FL MGUARD RS2000 TX/TX-B ... 107
6.1 Bedienelemente und Anzeigen ... 108
6.2 Inbetriebnahme ... 109
6.3 FL MGUARD RS2000 TX/TX-B installieren ... 110
6.4 Konfiguration vorbereiten ... 116
6.5 Serielle Schnittstelle ... 118
6.6 Neustart, Recovery-Prozedur und Flashen der Firmware ... 119
6.7 Technische Daten ... 125

7 FL MGUARD RS4000 TX/TX-P ... 127
7.1 Bedienelemente und Anzeigen ... 128
7.2 Inbetriebnahme ... 130
7.3 FL MGUARD RS4000 TX/TX-P installieren ... 131
7.4 Konfiguration vorbereiten ... 136
7.5 Konfiguration im Stealth-Modus ... 137
7.6 Lokale Konfigurationsverbindung herstellen ... 139
7.7 Fernkonfiguration ... 141
7.8 Serielle Schnittstelle ... 141
7.9 Neustart, Recovery-Prozedur und Flashen der Firmware ... 142

7.10 Technische Daten 147

8 FL MGUARD RS4000 TX/TX VPN-M 149

8.1 Bedienelemente und Anzeigen 150
8.2 Inbetriebnahme 152
8.3 FL MGUARD RS4000 TX/TX VPN-M installieren 153
8.4 Konfiguration vorbereiten 158
8.5 Konfiguration im Stealth-Modus 159
8.6 Lokale Konfigurationsverbindung herstellen 162
8.7 Fernkonfiguration 164
8.8 Serielle Schnittstelle 164
8.9 Neustart, Recovery-Prozedur und Flashen der Firmware 165
8.10 Technische Daten 170

9 FL MGUARD GT/GT 171

9.1 Bedienelemente und Anzeigen 172
9.2 Inbetriebnahme 176
9.3 FL MGUARD GT/GT installieren 177
9.4 Konfiguration vorbereiten 186
9.5 Lokale Konfigurationsverbindung herstellen 188
9.6 Fernkonfiguration 190
9.7 Serielle Schnittstelle 190
9.8 Neustart, Recovery-Prozedur und Flashen der Firmware 191
9.9 Technische Daten 197

10 FL MGUARD PCI(E)4000 201

10.1 Bedienelemente und Anzeigen 202
10.2 Inbetriebnahme 203
10.3 FL MGUARD PCI4000 installieren 204
10.4 Konfiguration vorbereiten 205
10.5 Konfiguration im Stealth-Modus 206
10.6 Lokale Konfigurationsverbindung herstellen 211
10.7 Fernkonfiguration 213
10.8 Neustart, Recovery-Prozedur und Flashen der Firmware 214
10.9 Technische Daten 218

11 FL MGUARD SMART2 219

11.1 Bedienelemente und Anzeigen 220
11.2 Inbetriebnahme 221

11.3 FL MGUARD SMART2 anschließen 222
11.4 Konfiguration vorbereiten 223
11.5 Konfiguration im Stealth-Modus 224
11.6 Lokale Konfigurationsverbindung herstellen 227
11.7 Fernkonfiguration 229
11.8 Neustart, Recovery-Prozedur und Flashen der Firmware 230
11.9 Technische Daten 234

12 FL MGUARD CENTERPORT 235
12.1 Bedienelemente und Anzeigen 236
12.2 Inbetriebnahme 237
12.3 FL MGUARD CENTERPORT installieren und booten 238
12.4 Konfiguration vorbereiten 243
12.5 Lokale Konfigurationsverbindung herstellen 244
12.6 Fernkonfiguration 246
12.7 Serielle Schnittstelle 246
12.8 Neustart, Recovery-Prozedur und Flashen der Firmware 247
12.9 Technische Daten 253

13 FL MGUARD DELTA TX/TX 255
13.1 Bedienelemente und Anzeigen 256
13.2 Inbetriebnahme 257
13.3 FL MGUARD DELTA TX/TX anschließen 258
13.4 Konfiguration vorbereiten 259
13.5 Konfiguration im Stealth-Modus 260
13.6 Lokale Konfigurationsverbindung herstellen 263
13.7 Fernkonfiguration 265
13.8 Serielle Schnittstelle 265
13.9 Neustart, Recovery-Prozedur und Flashen der Firmware 266
13.10 Technische Daten 271

14 IP-Adressen vergeben und DHCP/TFTP-Server einrichten 273
14.1 Vergabe der IP-Adresse mit IPAssign.exe 273
14.2 DHCP- und TFTP-Server installieren 276

1 Zu Ihrer Sicherheit

Lesen Sie dieses Handbuch sorgfältig und bewahren Sie es für späteres Nachschlagen auf.

1.1 Kennzeichnung der Warnhinweise

Dieses Symbol mit dem Signalwort **ACHTUNG** warnt vor Handlungen, die zu einem Sachschaden oder einer Fehlfunktion führen können.

Hier finden Sie zusätzliche Informationen oder weiterführende Informationsquellen.

1.2 Über dieses Handbuch

Folgende Elemente werden in diesem Handbuch verwendet:

Fett	Bezeichnung von Bedienelementen, Variablennamen oder sonstige Hervorhebungen
Kursiv	– Produkt-, Modul- oder Komponentenbezeichnungen (z. B. *tftpd64.exe*, *Config API*) – Fremdsprachliche Bezeichnungen oder Eigennamen – Sonstige Hervorhebungen
–	Unnummerierte Aufzählung
1.	Nummerierte Aufzählung
•	Handlungsanweisung
⇒	Ergebnis einer Handlung

1.3 Qualifikation der Benutzer

Der in diesem Handbuch beschriebene Produktgebrauch richtet sich ausschließlich an

– Elektrofachkräfte oder von Elektrofachkräften unterwiesene Personen. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.
– Qualifizierte Anwendungsprogrammierer und Software-Ingenieure. Die Anwender müssen vertraut sein mit den einschlägigen Sicherheitskonzepten zur Automatisierungstechnik sowie den geltenden Normen und sonstigen Vorschriften.

1.4 Bestimmungsgemäße Verwendung

– Die Geräte der Serie FL MGUARD sind industrietaugliche Security-Router mit integrierter Stateful-Packet-Inspection-Firewall und optionalem IPsec- und OpenVPN. Sie eignen sich für die dezentrale Absicherung von Produktionszellen oder einzelner Maschinen gegen Manipulationen sowie für Fernwartungsszenarien. Die Geräte sind mit einem hohen Anspruch an die dezentrale Sicherheit und Hochverfügbarkeit konzipiert.

1.5 Veränderung des Produkts

Öffnen oder Verändern des Gerätes ist nicht zulässig. Reparieren Sie das Gerät nicht selbst, sondern ersetzen Sie es durch ein gleichwertiges Gerät. Reparaturen dürfen nur vom Hersteller vorgenommen werden. Der Hersteller haftet nicht für Schäden aus Zuwiderhandlung.

1.6 Sicherheitshinweise

ACHTUNG: Installation nur durch qualifiziertes Personal

Die Installation, Inbetriebnahme und Wartung des Produkts darf nur durch ausgebildetes Fachpersonal erfolgen, das vom Anlagenbetreiber dazu autorisiert wurde. Elektrofachkraft ist, wer aufgrund seiner fachlichen Ausbildung, Kenntnisse und Erfahrungen sowie Kenntnis der einschlägigen Normen die ihm übertragenen Arbeiten beurteilen und mögliche Gefahren erkennen kann. Das Fachpersonal muss diese Dokumentation gelesen und verstanden haben und die Anweisungen befolgen. Beachten Sie die geltenden nationalen Vorschriften für Betrieb, Funktionsprüfung, Reparatur und Wartung von elektronischen Geräten.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerkanschlüsse des Geräts nur an Ethernet-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

ACHTUNG: Elektrostatische Entladung

Die Geräte enthalten Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können. Beachten Sie beim Umgang mit den Geräten die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) gemäß EN 61340-5-1 und EN 61340-5-2.

ACHTUNG: Anforderung an die Spannungsversorgung

Tragschienengeräte sind ausschließlich für den Betrieb mit Sicherheitskleinspannung (SELV/PELV) ausgelegt. Im redundanten Betrieb müssen beide Spannungsversorgungen den Anforderungen der Sicherheitskleinspannung genügen.

ACHTUNG: Anforderung an den Schaltschrank/Schaltkasten

Tragschienengeräte werden innerhalb eines Schaltschranks oder -kastens auf eine Norm-Tragschiene aufgerastet. Dieser Schaltschrank/-kasten muss den Anforderungen der IEC/EN 62368-1 bez. der Brandschutzumhüllung genügen.

ACHTUNG: Anforderung an die Funktionserdung

Montieren Sie Tragschienengeräte auf einer geerdeten Tragschiene. Die Erdung des Moduls erfolgt mit dem Aufrasten auf die Tragschiene.

ACHTUNG: Anforderung an den Montageort

- Die vorgeschriebene Einbaulage von Tragschienengeräten ist senkrecht auf einer horizontal montierten Tragschiene. Die Lüftungsschlitze dürfen nicht bedeckt werden, so dass die Luft frei zirkulieren kann. Als Abstand zu den Lüftungsschlitzen des Gehäuses werden mindestens 3 cm empfohlen.
- Die Schutzart IP20 (IEC 60529-0/EN 60529-0) des Gerätes ist für eine saubere und trockene Umgebung vorgesehen. Setzen Sie das Gerät keiner mechanischen und/oder thermischen Beanspruchung aus, die die beschriebenen Grenzen überschreitet.
- Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigung

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

1.6.1 UL-/HazLoc-Informationen

- This equipment is an open-type device meant to be installed in an enclosure suitable for the environment that is only accessible with the use of a tool.
- Suitable for use in class I, division 2, groups A, B, C and D hazardous locations, or non-hazardous locations only.
- WARNING - Explosion Hazard - Substitution of any components may impair suitability for Class I, Division 2.
- WARNING - Explosion Hazard - Do not disconnect equipment while the circuit is live or unless the area is known to be free of ignitable concentrations.
- AVERTISSEMENT - Risque d'explosion - Tout remplacement d'un composant peut entraver la fiabilité pour Classe I, Division 2. components may impair suitability for Class I, Division 2.
- AVERTISSEMENT - Risque d'explosion - Ne pas déconnecter l'équipement lorsque le circuit est sous tension ou sauf si la zone est connue pour être exempte de concentrations inflammables.

1.7 IT-Sicherheit

Sie müssen Komponenten, Netzwerke und Systeme vor unberechtigten Zugriffen schützen und die Datenintegrität gewährleisten. Hierzu müssen Sie bei netzwerkfähigen Geräten, Lösungen und PC-basierter Software organisatorische und technische Maßnahmen ergreifen.

Phoenix Contact empfiehlt dringend den Einsatz eines Managementsystems für Informationssicherheit (ISMS) zur Verwaltung aller infrastrukturellen, organisatorischen und personellen Maßnahmen, die zur Erhaltung der Informationssicherheit notwendig sind.

Darüber hinaus empfiehlt Phoenix Contact, mindestens die folgenden Maßnahmen zu berücksichtigen.

Weiterführende Informationen zu den im Folgenden genannten Maßnahmen erhalten Sie auf den folgenden Webseiten (letzter Zugriff am 13.09.2022):

– bsi.bund.de/it-sik.html

– ics-cert.us-cert.gov/content/recommended-practices

Verwenden Sie die jeweils aktuelle Firmware-Version

Phoenix Contact stellt regelmäßig Firmware-Updates zur Verfügung. Verfügbare Firmware-Updates finden Sie auf der Produktseite des jeweiligen Geräts.

- Stellen Sie sicher, dass die Firmware aller verwendeten Geräte immer auf dem aktuellen Stand ist.
- Beachten Sie die Change Notes / Release Notes zur jeweiligen Firmware-Version.
- Beachten Sie die Webseite des Product Security Incident Response Teams (PSIRT) von Phoenix Contact für Sicherheitshinweise zu veröffentlichten Sicherheitslücken.

Verwenden Sie aktuelle Sicherheits-Software

- Um Sicherheitsrisiken wie Viren, Trojaner und andere Schad-Software zu erkennen und auszuschalten, installieren Sie auf allen PCs eine Sicherheits-Software.
- Stellen Sie sicher, dass die Sicherheits-Software immer auf dem aktuellen Stand ist und die neuesten Datenbanken nutzt.
- Nutzen Sie Whitelist-Tools zur Überwachung des Gerätekontexts.
- Um die Kommunikation Ihrer Anlage zu prüfen, nutzen Sie ein Intrusion-Detection-System.

Führen Sie regelmäßige Bedrohungsanalysen durch

- Um festzustellen, ob die von Ihnen getroffenen Maßnahmen Ihre Komponenten, Netzwerke und Systeme noch ausreichend schützen, ist eine regelmäßige Bedrohungsanalyse erforderlich.
- Führen Sie regelmäßige Bedrohungsanalysen durch.

Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Um Ihre Komponenten, Netzwerke und Systeme zu schützen, ist es nicht ausreichend, isoliert betrachtete Maßnahmen zu ergreifen. Defense-in-Depth-Mechanismen umfassen mehrere, aufeinander abgestimmte und koordinierte Maßnahmen, die Betreiber, Integratoren und Hersteller miteinbeziehen.

- Berücksichtigen Sie bei der Anlagenplanung Defense-in-depth-Mechanismen

Deaktivieren Sie nicht benötigte Kommunikationskanäle

- Deaktivieren Sie nicht benötigte Kommunikationskanäle (z. B. SNMP, FTP, BootP, DCP etc.) an den von Ihnen eingesetzten Komponenten.

Binden Sie Komponenten und Systeme nicht in öffentliche Netzwerke ein

- Vermeiden Sie es, Komponenten und Systeme in öffentliche Netzwerke einzubinden.
- Wenn Sie Ihre Komponenten und Systeme über ein öffentliches Netzwerk erreichen müssen, verwenden Sie ein VPN (Virtual Private Network).

Beschränken Sie die Zugangsberechtigung zum Gerät

- Vermeiden Sie, dass unberechtigte Personen physischen Zugriff auf das Gerät erlangen. Ein Zugriff auf die Hardware des Geräts könnte es einem Angreifer ermöglichen, die Sicherheitsfunktionen zu manipulieren.
- Beschränken Sie die Zugangsberechtigung zu Komponenten, Netzwerken und Systemen auf die Personen, für die eine Berechtigung unbedingt notwendig ist.
- Deaktivieren Sie nicht genutzte Benutzerkonten.

Sichern Sie den Zugriff ab

- Ändern Sie voreingestellte Passwörter während der ersten Inbetriebnahme.
- Verwenden Sie sichere Passwörter, deren Komplexität und Lebensdauer dem Stand der Technik entsprechen (z. B. mit einer Länge von mindestens zehn Zeichen und einer Mischung aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen).
- Verwenden Sie Passwort-Manager mit zufällig erzeugten Passwörtern.
- Ändern Sie Passwörter entsprechend der für Ihre Anwendung geltenden Regeln.
- Verwenden Sie, sofern möglich, zentrale Benutzerverwaltungen zur Vereinfachung des User Managements und der Anmeldeinformationen.

Verwenden Sie bei Fernzugriff sichere Zugriffswege

- Verwenden Sie für einen Fernzugriff sichere Zugriffswege wie VPN (Virtual Private Network) oder HTTPS.

Verwenden Sie eine Firewall

- Richten Sie eine Firewall ein, um Ihre Netzwerke und darin eingebundene Komponenten und Systeme vor ungewollten Netzwerkzugriffen zu schützen.
- Verwenden Sie eine Firewall, um ein Netzwerk zu segmentieren oder bestimmte Komponenten (z. B. Steuerungen) zu isolieren.

Aktivieren Sie eine sicherheitsrelevante Ereignisprotokollierung (Logging)

- Aktivieren Sie die sicherheitsrelevante Ereignisprotokollierung (Logging) gemäß der Sicherheitsrichtlinie und der gesetzlichen Bestimmungen zum Datenschutz.

Schützen Sie den Zugriff auf die SD-Karte

Geräte mit SD-Karten benötigen Schutz gegen unerlaubte physische Zugriffe. Eine SD-Karte kann mit einem herkömmlichen SD-Kartenleser jederzeit ausgelesen werden. Wenn Sie die SD-Karte nicht physisch gegen unbefugte Zugriffe schützen (z. B. mithilfe eines gesicherten Schaltschranks), sind somit auch sensible Daten für jeden abrufbar.

- Stellen Sie sicher, dass Unbefugte keinen Zugriff auf die SD-Karte haben.
- Stellen Sie bei der Vernichtung der SD-Karte sicher, dass die Daten nicht wiederhergestellt werden können.

1.8 Aktuelle Sicherheitshinweise zu Ihrem Produkt

Product Security Incident Response Team (PSIRT)

Das Phoenix Contact PSIRT ist das zentrale Team für Phoenix Contact und dessen Tochterunternehmen, dessen Aufgabe es ist, auf potenzielle Sicherheitslücken, Vorfälle und andere Sicherheitsprobleme im Zusammenhang mit Produkten, Lösungen sowie Diensten von Phoenix Contact zu reagieren.

Das Phoenix Contact PSIRT leitet die Offenlegung, Untersuchung und interne Koordination und veröffentlicht Sicherheitshinweise zu bestätigten Sicherheitslücken, bei denen Maßnahmen zur Abschwächung oder Behebung verfügbar sind.

Die PSIRT-Webseite (phoenixcontact.com/psirt) wird regelmäßig aktualisiert. Zusätzlich empfiehlt Phoenix Contact, den PSIRT-Newsletter zu abonnieren.

Jeder kann per E-Mail Informationen zu potenziellen Sicherheitslücken beim Phoenix Contact PSIRT einreichen.

1.9 Support

Zusätzliche Informationen zum Gerät sowie Release Notes, Anwenderhilfen und Software-Updates finden Sie unter folgender Internet-Adresse: phoenixcontact.net/product/<Artikelnummer>.

Bei Problemen mit Ihrem Gerät oder der Bedienung Ihres Geräts wenden Sie sich bitte an Ihre Bezugsquelle.

Um in einem Fehlerfall schnelle Hilfe zu erhalten, erstellen Sie, falls möglich, beim Auftreten des Fehlers umgehend einen Snapshot der Gerätekonfiguration, den Sie dem Support zur Verfügung stellen können.

Für weitergehende Informationen zur Verwendung von Snapshots siehe mGuard-Anwenderhandbuch (UM DE MGUARD), erhältlich unter phoenixcontact.net/products oder help.mguard.com.

2 FL MGUARD RS4000/RS2000

Tabelle 2-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD RS4000 TX/TX	2700634
FL MGUARD RS4000 TX/TX VPN	2200515
FL MGUARD RS2000 TX/TX VPN	2700642

Produktbeschreibung

Der **FL MGUARD RS4000** ist ein Security-Router mit intelligenter Firewall und optionalem IPsec-VPN (optional bis zu 10 oder 250 Tunnel). Er ist für den Einsatz in der Industrie mit hohen Ansprüchen an die dezentrale Sicherheit und die Hochverfügbarkeit konzipiert.

Der **FL MGUARD RS2000** ist eine Variante mit einfacher Firewall und integriertem IP-Sec-VPN (maximal zwei Tunnel). Der Funktionsumfang ist auf das Wesentliche reduziert. Er eignet sich für sichere Fernwartungsszenarien in der Industrie und ermöglicht eine schnelle Inbetriebnahme von robusten, industrietauglichen Feldgeräten für einen störungsfreien, autarken Betrieb.

Beide Varianten unterstützen einen auswechselbaren Konfigurationsspeicher in Form einer SD-Karte. (Die SD-Karten sind nicht im Lieferumfang enthalten). Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

Folgende Anschlussmöglichkeiten stehen zur Verfügung:

FL MGUARD RS4000: (LAN/WAN)	FL MGUARD RS2000: (LAN/WAN)
TX/TX Ethernet/Ethernet	TX/TX VPN Ethernet/Ethernet + VPN
TX/TX VPN Ethernet/Ethernet + VPN	

Bild 2-1 FL MGUARD RS4000/FL MGUARD RS2000

2.1 Bedienelemente und Anzeigen

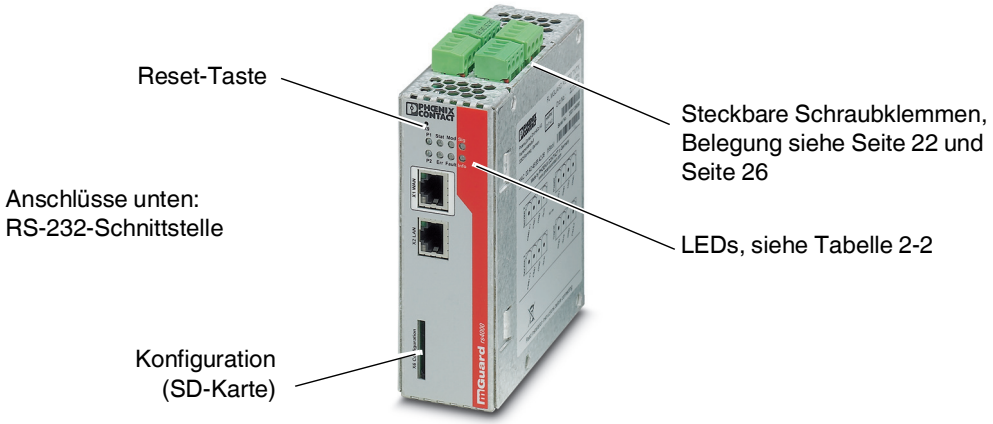


Bild 2-2 Bedienelemente und Anzeigen des FL MGUARD RS4000

Tabelle 2-2 Anzeigen und LED-Blinkverhalten des FL MGUARD RS4000/RS2000

LED	Zustand		Bedeutung
P1	Grün	Ein	Stromversorgung 1 ist aktiv
P2	Grün	Ein	Stromversorgung 2 ist aktiv (FL MGUARD RS2000: unbelegt)
STAT	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
ERR	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Reset-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe Seite 35) oder wenden Sie sich an Ihren Händler.
STAT+ ERR	Abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
SIG	–		(nicht belegt)
FAULT	Rot	Ein	Der Meldeausgang nimmt aufgrund eines Fehlers Low-Pegel ein (invertierte Logik) (siehe Seite 24 oder Seite 25). Während eines Neustarts ist der Meldeausgang inaktiv.
MOD	Grün	Ein	Verbindung per Modem hergestellt

Tabelle 2-2 Anzeigen und LED-Blinkverhalten des FL MGUARD RS4000/RS2000[...]

LED	Zustand		Bedeutung
INFO	Grün	Ein	Bis Firmware-Version 8.0: Konfigurierte VPN-Verbindung ist aufgebaut Ab Firmware-Version 8.1 Konfigurierte VPN-Verbindungen sind aufgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze sind eingeschaltet
		Blinkt	Bis Firmware-Version 8.0: Konfigurierte VPN-Verbindung wird auf- oder abgebaut Ab Firmware-Version 8.1: Konfigurierte VPN-Verbindungen werden auf- oder abgebaut oder die definierten Firewall-Regelsätze werden ein- oder ausgeschaltet
LAN	Grün	Ein	Die LAN/WAN LEDs befinden sich in den LAN/WAN-Buchsen (10/100 und Duplex-Anzeige) **Ethernet-Status**. Zeigt den Status des LAN- bzw. WAN-Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
WAN	Grün	Ein	

2.2 Inbetriebnahme

2.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss der mGuard richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des mGuards nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuards verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

– Umgebungstemperatur:
  -20°C ... +60°C
– Maximale Luftfeuchtigkeit, nicht kondensierend:
  5 % ... 95 %

Setzen Sie den mGuard keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

2.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

– Das Gerät
– Packungsbeilage
– Steckbare Schraubklemmen für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

2.3 FL MGUARD RS4000/RS2000 installieren

2.3.1 Montage/Demontage

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

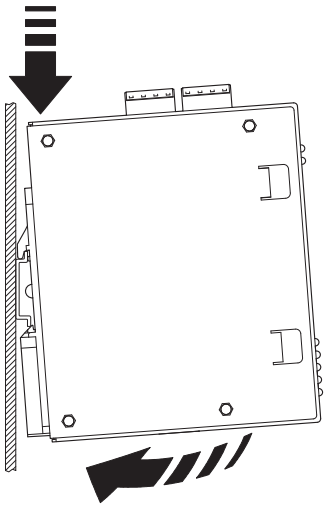


Bild 2-3 Montage des das Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein. Drücken Sie das Gerät dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

2.3.2 Netzwerkverbindung anschließen

ACHTUNG: Schließen Sie die Netzwerk-Ports des mGuards nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des mGuards verbunden werden.

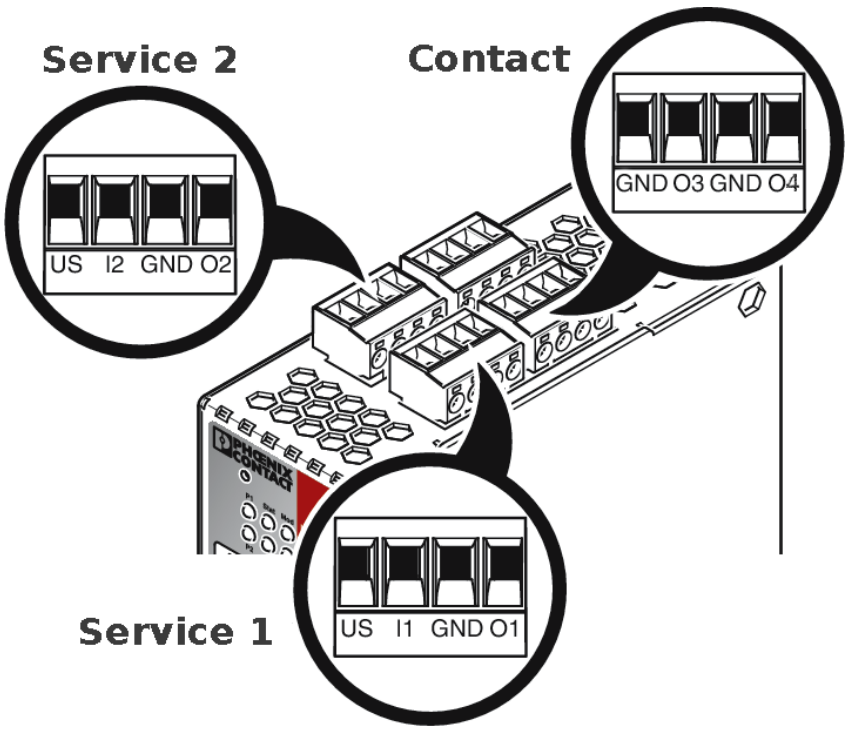
- Verbinden Sie den mGuard mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN 1 des mGuards mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

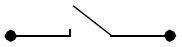
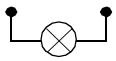
2.3.3 Servicekontakte

ACHTUNG: Schließen Sie die Spannungs- und Masseausgänge **US** (bzw. **CMD V+**) und **GND nicht** an eine externe Spannungsquelle an.

Beachten Sie, dass mit der Firmware-Version bis einschließlich 7.6.x nur die Kontakte „Service 1“ belegt sind. Die Kontakte „Service 2“ sind ab der Firmware-Version 8.1 verfügbar.

Die steckbaren Schraubklemmen der Servicekontakte können während des Betriebs des mGuards entfernt oder aufgesetzt werden.



Service 1 + 2	US	I1/I2	GND	O1/O2
	Spannungsausgang (+) Versorgungsspannung	Schalteingang 11...36 V DC	Masseausgang (-) Versorgungsspannung	Kurzschlussfester Schaltausgang *
	Beispiel 		Beispiel 	

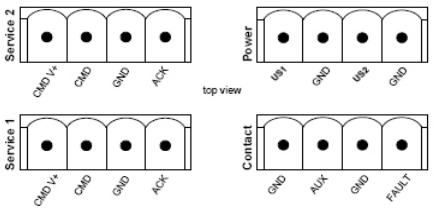
Power	24V	0V	24V	0V
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 2.3.4		nur beim FL MGUARD RS4000 siehe Kapitel 2.3.4	

Contact	GND	O3	GND	O4
	nicht verwendet	nicht verwendet	Meldeausgang (-)	Meldeausgang (+)†

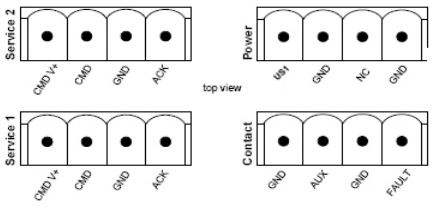
* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

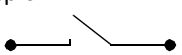
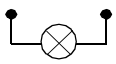
Die nachfolgend beschriebene Bezeichnung der Kontakte ist ebenfalls möglich:



FL MGUARD RS4000



FL MGUARD RS2000

Service 1 + 2	CMD V+	CMD	GND	ACK
	Spannungsausgang (+) Versorgungsspannung	Schalteingang 11...36 V DC	Masseausgang (-) Versorgungsspannung	Kurzschlussfester Schaltausgang *
	Beispiel 		Beispiel 	

Power	US1	GND	US2	GND
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 2.3.4		nur beim FL MGUARD RS4000 siehe Kapitel 2.3.4	

Contact	GND	AUX	GND	FAULT
	nicht verwendet	nicht verwendet	Meldeausgang (-)	Meldeausgang (+)†

* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Zwischen die **Servicekontakte US** und **I** (bzw. CMD V+ und CMD) kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Die Kontakte **O1/O2 (+)** und **O4 (+)** (bzw. ACK und FAULT) sind potenzialbehaftet, dauerkurzschlussfest und liefern jeweils maximal 250 mA.

Die Schalteingänge und Schaltausgänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen von SPS-Steuerungen. Achten Sie in diesem Fall auf ein gleiches Potenzial und die Spannungs- und Stromangaben.

Die Servicekontakte können je nach verwendeter Firmware-Version für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

Servicekontakte ab Firmware-Version 8.1

Eingang/CMD I1, CMD I2

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob an die Eingänge ein Taster oder ein Ein-/Aus-Schalter angeschlossen wurde. Es können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze über den entsprechenden Schalter geschaltet werden. Auch eine Mischung von VPN-Verbindungen und Firewall-Regelsätzen ist möglich. Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und welche Firewall-Regelsätze an diesen Eingang gebunden sind.

Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von zuvor definierten VPN-Verbindungen oder der definierten Firewall-Regelsätze.

Bedienung eines angeschlossenenTasters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf EIN stellen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf AUS stellen.

Meldekontakt (Meldeausgang) O1, O2 bzw. ACK

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht und über die LED Info 1 (Ausgang/O1 bzw. ACK) oder LED Info 2 (Ausgang/O2 bzw. ACK) angezeigt werden.

Wenn VPN-Verbindungen überwacht werden, zeigt eine leuchtende LED Info, dass diese VPN-Verbindungen bestehen.

Alarmausgang O4 bzw. FAULT

Der Alarmausgang O4 überwacht die Funktion des Geräts und ermöglicht damit eine Ferndiagnose.

Die LED Fault leuchtet rot, wenn der Meldeausgang aufgrund eines Fehlers Low-Pegel einnimmt (invertierte Logik).

Durch den Alarmausgang O4 wird folgendes gemeldet, wenn das unter „Verwaltung >> Service I/O >> Alarmausgang“ aktiviert worden ist.

- Der Ausfall der redundanten Versorgungsspannung
- Überwachung des Link-Status der Ethernet-Anschlüsse
- Überwachung des Temperaturzustandes
- Überwachung des Redundanzstatus
- Überwachung des Verbindungsstatus des internen Modems

Servicekontakte bis Firmware-Version 8.0

Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau einer zuvor definierten VPNVerbindung.

Der Ausgang signalisiert den Status der VPN-Verbindung (in der Web-Oberfläche unter „IPsec VPN >> Global“ unter „Optionen“).

Bedienung eines angeschlossenenTasters

- Zum Aufbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis die LED INFO blinkt. Erst dann den Taster loslassen.

  Das Blinken signalisiert, dass der mGuard das Kommando zum Aufbau der VPN-Verbindung erhalten hat und dabei ist, die VPN-Verbindung aufzubauen. Sobald die VPNVerbindung steht, leuchtet die LED INFO kontinuierlich.
- Zum Abbau der VPN-Verbindung den Taster einige Sekunden gedrückt halten, bis der Signal-Ausgang blinkt oder erlischt. Erst dann den Taster loslassen.

  Sobald die LED INFO nicht mehr leuchtet, ist die VPN-Verbindung abgebaut.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Aufbau der VPN-Verbindung den Schalter auf EIN stellen.
- Zum Abbau der VPN-Verbindung den Schalter auf AUS stellen.

LED INFO

Wenn die LED INFO nicht leuchtet, wird dadurch generell signalisiert, dass die definierte VPN-Verbindung nicht besteht. Die VPN-Verbindung wurde entweder nicht aufgebaut oder ist wegen eines Fehlers ausgefallen.

Wenn die LED INFO leuchtet, besteht die VPN-Verbindung.

Wenn die LED INFO blinkt, wird die VPN-Verbindung gerade auf- oder abgebaut.

Meldekontakt (Meldeausgang)

Der Meldekontakt überwacht die Funktion des Geräts und ermöglicht damit eine Ferndiagnose.

Die LED FAULT leuchtet rot, wenn der Meldeausgang aufgrund eines Fehlers Low-Pegel einnimmt.

Bei dem Meldekontakt entspricht die Spannung der angelegten Versorgungsspannung. Bei der Überwachung der Ausgangsspannung wird folgendes gemeldet:

- Der Ausfall mindestens einer der beiden Versorgungsspannungen.
- Eine Unterschreitung des Grenzwertes bei der Stromversorgung des Geräts (Versorgungsspannung 1 und/oder 2 ist kleiner als 11 V).
- Überwachung des Link-Status der Ethernet-Anschlüsse, wenn dies konfiguriert worden ist. Im Lieferzustand wird die Verbindung nicht überwacht. Sie können die Überwachung einstellen (in der Web-Oberfläche unter „Verwaltung >> Systemeinstellung >> Meldekontakt“).
- Ein Fehler beim Selbsttest.

Während eines Neustarts ist der Meldekontakt abgeschaltet, bis das Gerät vollständig den Betrieb aufgenommen hat. Das gilt auch, wenn der Meldekontakt in der Software-Konfiguration unter „Manuelle Konfiguration“ auf „Geschlossen“ gestellt ist.

2.3.4 Versorgungsspannung anschließen

WARNUNG: Das Gerät ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach IEC 60950/EN 60950/VDE 0805 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über eine steckbare Schraubklemme, die sich oben auf dem Gerät befindet.

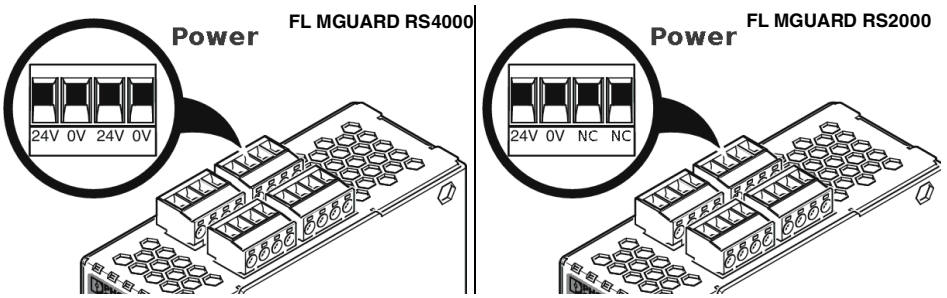


Bild 2-4 Versorgungsspannung anschließen

Anstatt der Bezeichnung **24V/24V** wird die Bezeichnung **US1/US2** ebenfalls verwendet.

Der **FL MGUARD RS4000** hat eine redundante Versorgungsspannung. Wenn Sie nur eine Versorgungsspannung anschließen, erhalten Sie eine Fehlermeldung.

- Nehmen Sie die steckbaren Schraubklemmen für Stromversorgung und Servicekontakte ab.
- Schließen Sie die Servicekontakte nicht an eine externe Spannungsquelle an.
- Verdrahten Sie die Versorgungsspannungsleitungen mit der entsprechenden Schraubklemme **24V/24V** (bzw. US1/US2) des Geräts. Ziehen Sie die Schrauben der Schraubklemmen mit 0,5 ... 0,8 Nm an.
- Stecken Sie die Schraubklemmen auf die vorgesehenen Buchsen auf der Oberseite des Geräts (siehe Bild 2-4).

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist. Beim FL MGUARD RS4000 leuchtet zusätzlich die Status-Anzeige P2 bei redundantem Anschluss der Versorgungsspannung.

Das Gerät bootet die Firmware. Die Status-Anzeige STAT blinkt grün. Das Gerät ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die Status-Anzeigen P1/P2 grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

Redundante Spannungsversorgung (FL MGUARD RS4000)

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den FL MGUARD RS4000 alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der FL MGUARD RS4000 über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge **24V/24V** (bzw. US1/US2) zuführen oder eine geeignete Drahtbrücke zwischen den Anschlüssen **24V und 24V** (bzw. US1 und US2) anbringen.

2.4 Konfiguration vorbereiten

2.4.1 Anschlussvoraussetzungen

– Das Gerät muss an mindestens einem aktiven Netzteil angeschlossen sein.
– **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
– **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
– Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

2.4.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS-Verfahren (Easy-Initial-Setup) eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen ohne Verbindung mit einem externen Netzwerk.

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 2-3 Voreingestellte Adressen

Werkseinstellung	Netz-werk-Modus	Management-IP #1	Management-IP #2
FL MGUARD RS4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät ist auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. Wenn Sie VPN-Verbindungen nutzen wollen, müssen Sie eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe Seite 31). Alternativ können Sie eine andere Stealth-Konfiguration wählen oder einen anderen Netzwerk-Modus verwenden.

2.5 Konfiguration im Stealth-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter zwei IP-Adressen erreichbar:

– https://192.168.1.1/ (siehe Seite 29)
– https://1.1.1.1/ (siehe Seite 29)

Alternativ kann per BootP eine IP-Adresse zugewiesen werden (siehe „IP-Adresse per BootP zuweisen“ auf Seite 30).

Das Gerät ist unter der Adresse https://192.168.1.1/ erreichbar, wenn die externe Netzwerkschnittstelle beim Starten nicht verbunden ist.

Das Gerät kann von Rechnern über https://1.1.1.1/ erreicht werden, wenn diese direkt oder indirekt am LAN-Port des Geräts angeschlossen sind. Dazu muss das Gerät mit LAN- und WAN-Port in ein funktionierendes Netzwerk eingebunden sein, bei dem das Standard-Gateway über den WAN-Port erreichbar ist.

– Nach einem Zugriff über die IP-Adresse 192.168.1.1 und einer erfolgreichen Anmeldung wird die IP-Adresse 192.168.1.1 als Management IP-Adresse fest eingestellt.
– Nach einem Zugriff über die IP-Adresse 1.1.1.1 oder nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

2.5.1 IP-Adresse 192.168.1.1

Im Stealth-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.

- Das Gerät ist im Auslieferungszustand.
- Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
- Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

2.5.2 IP-Adresse https://1.1.1.1/

Bei konfigurierter Netzwerkschnittstelle

Damit das Gerät über die Adresse **https://1.1.1.1/** angesprochen werden kann, muss er an eine konfigurierte Netzwerkschnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt und dabei das Standard-Gateway über den WAN-Port des Geräts erreichbar ist.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des mGuard-Geräts herstellen (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 31). Fahren Sie in diesem Falle dort fort.

Nach einem Zugriff über die IP-Adresse 1.1.1.1 steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

2.5.3 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

In Kapitel 14.1 wird die IP-Adressvergabe mit Hilfe der kostenlosen Windows-Software „IP Assignment Tool“ (IPAssign.exe) erklärt.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald das Gerät eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem das Gerät eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit das Gerät erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash) ausgeführt werden.

2.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgenden Adressen erreichbar:

Tabelle 2-4 Voreingestellte Adressen

Werkseinstellung	Netz-werk-Modus	Management-IP #1	Management-IP #2
FL MGUARD RS4000	Stealth	https://1.1.1.1/	https://192.168.1.1/
FL MGUARD RS2000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme mit dem Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die IP-Adresse des Geräts vollständig ein (siehe Tabelle 2-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 35).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.
  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.
  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst-unterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 2-5 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

2.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an, unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

2.8 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

2.9 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

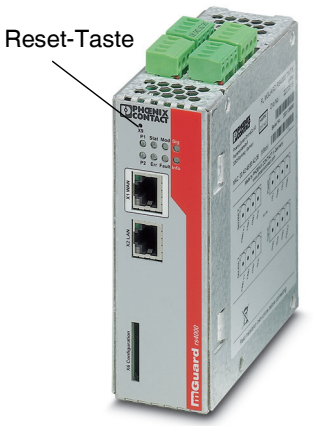


Bild 2-6 Reset-Taste

2.9.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED ERR leuchtet (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

2.9.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 2-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät wird in den Stealth-Modus mit der Werkseinstellung „mehrere Clients“ zurückgesetzt.

– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
– Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Das Gerät befindet sich im Router- oder PPPoE-Modus.
– Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
– Sie kennen die aktuelle IP-Adresse des Geräts nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 2-6 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED STAT grün.
- Wenn die LED STAT grün erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED STAT grün
  Bei Misserfolg leuchtet die LED ERR rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

2.9.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ist auf dem Gerät die mGuard-Firmwareversion 5.0.0 oder höher installiert, bleiben die auf dem Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

- alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
- diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

- Sie haben die mGuard-Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
- Diese SD-Karte ist in das Gerät eingesetzt.
- Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:

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

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs STAT, MOD und SIG grün leuchten. Dann ist der mGuard im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED Stat blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs STAT, MOD und SIG bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flash-Speicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED STAT leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, blinken die LEDs STAT, MOD und SIG gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie es neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 31).

2.10 Technische Daten

Hardware-Eigenschaften	FL MGUARD RS4000	FL MGUARD RS2000
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN-Port I 1 WAN-Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX	1 LAN-Port I 1 WAN-Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	Seriell RS-232 I D-SUB 9-Stecker je 2 digitale Ein- und Ausgänge	Seriell RS-232 I D-SUB 9-Stecker je 2 digitale Ein- und Ausgänge
Speicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher
Redundanz-Optionen	optional: VPN I Router und Firewall	nicht verfügbar
Stromversorgung	Spannungsbereich 11 ... 36 V DC, redundant	Spannungsbereich 11 ... 36 V DC
Leistungsaufnahme	typisch 2,13 Watt	typisch 2,13 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20	IP20
Temperaturbereich	-20 °C ... +60 °C (Betrieb) -20 °C ... +60 °C (Lagerung)	-20 °C ... +60 °C (Betrieb) -20 °C ... +60 °C (Lagerung)
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	725 g (TX/TX)	725 g (TX/TX)
Gewicht (inkl. Verpackung)	900 g (TX/TX)	900 g (TX/TX)

Firmware und Leistungswerte	FL MGUARD RS4000	FL MGUARD RS2000
Firmware-Kompatibilität	mGuard v7.4.0 oder höher; Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt	
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s	
Virtual Private Network (VPN)	IPsec (IETF-Standard) optional bis zu 250 VPN-Tunnel	IPsec (IETF-Standard) bis zu 2 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 20 MBit/s	
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software	
Diagnose	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) Meldekontakte I Servicekontakte I Log-File I Remote-Syslog	LEDs (Power, State, Error, Signal, Fault, Modem, Info) Meldekontakte I Servicekontakte I Log-File I Remote-Syslog

Sonstiges	FL MGUARD RS4000	FL MGUARD RS2000
Konformität	CE I FCC I UL 508 ANSI/ISA 12.12 Class I Div. 2	
Besonderheiten	Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Remote Services Portal ready	

3 FL MGUARD RS4004/RS2005

Tabelle 3-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD RS4004 DTX/TX	2701876
FL MGUARD RS4004 TX/TX VPN	2701877
FL MGUARD RS2005 TX VPN	2701875

Produktbeschreibung

Der **FL MGUARD RS4004** eignet sich für die dezentrale Absicherung von Produktionszellen oder einzelnen Maschinen gegen Manipulationen.

Er verfügt über einen 4-Port managed LAN-Switch, einen WAN- und einen DMZ-Port sowie über eine serielle Schnittstelle.

Die serielle Schnittstelle kann u. a. als Wegeredundanz zur WAN-Schnittstelle geschaltet werden. Ein dedizierter DMZ-Port mit eigenen Firewall-Regeln ermöglicht eine Segmentierung und differenziertere Sicherheitskonzepte. Sie können Automatisierungsgeräte mit seriellen Schnittstellen in Netzwerke einbinden, da ein COM-Server integriert ist.

Für eine software-unabhängige Fernwartung kann der FL MGUARD RS4004 als VPN-Router für optional bis zu 250 parallele, IPsec-verschlüsselte VPN-Tunnel eingesetzt werden.

Der **FL MGUARD RS2005** ist eine Variante mit einfacher Firewall und kann als VPN-Client für bis zu zwei parallele, IPsec-verschlüsselte VPN-Tunnel eingesetzt werden. Er eignet sich für sichere Fernwartungsszenarien und ermöglicht die Anbindung weltweit verteilter Maschinen und Steuerungen.

Beide Varianten unterstützen einen wechselbaren Konfigurationsspeicher in Form einer SD-Karte. Zur Erhöhung der Sicherheit können VPN-Verbindungen per Schaltkontakt oder Software-Schnittstelle ein- bzw. ausgeschaltet werden. Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

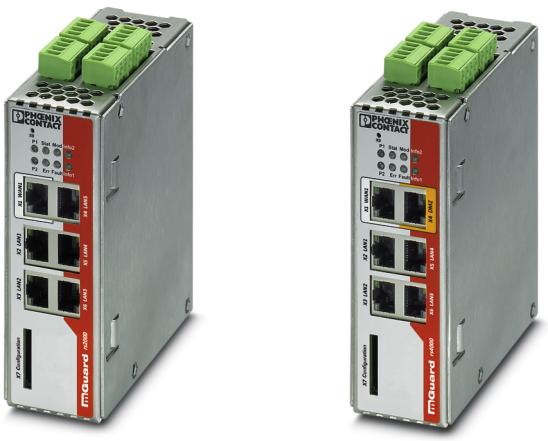


Bild 3-1 FL MGUARD RS2005/FL MGUARD RS4004

3.1 Bedienelemente und Anzeigen

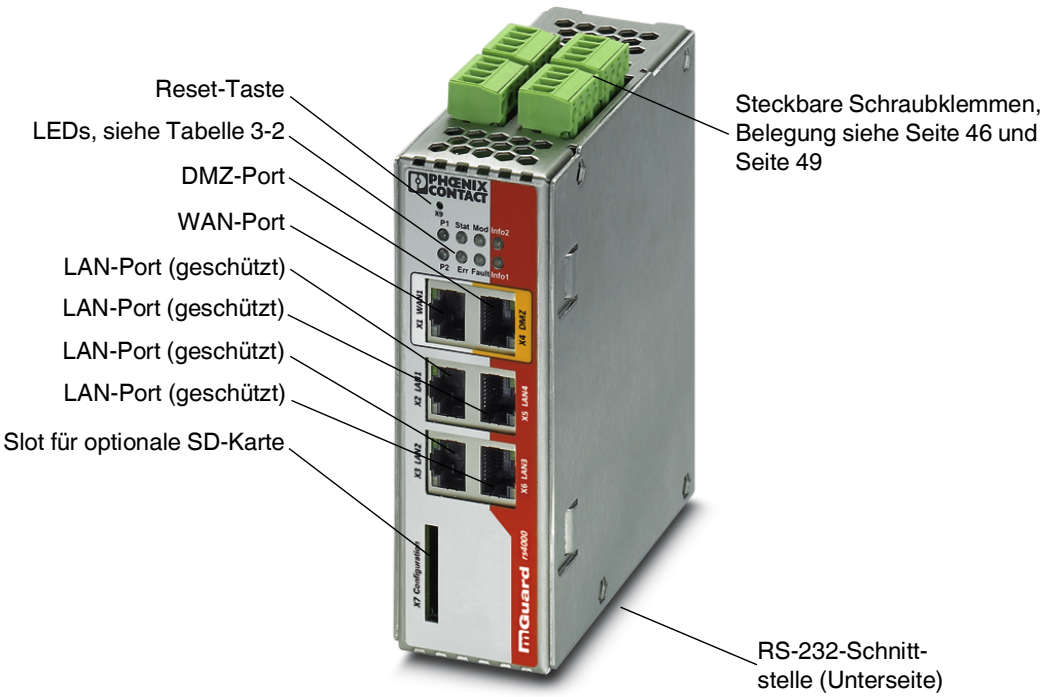


Bild 3-2 Bedienelemente und Anzeigen des FL MGUARD RS4004

Tabelle 3-2 Anzeigen des FL MGUARD RS4004/RS2005

LED	Zustand		Bedeutung
P1	Grün	Ein	Stromversorgung 1 ist aktiv
P2	Grün	Ein	Stromversorgung 2 ist aktiv (FL MGUARD RS2005: unbelegt)
Stat	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
Err	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Reset-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe Seite 55) oder wenden Sie sich an Ihren Händler.
Stat + Err	Abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Spannungsversorgung. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
Mod	Grün	Ein	Verbindung per Modem hergestellt
Fault	Rot	Ein	Der Meldeausgang nimmt aufgrund eines Fehlers Low-Pegel ein (invertierte Logik). Während eines Neustarts ist der Meldeausgang inaktiv.

Tabelle 3-2 Anzeigen des FL MGUARD RS4004/RS2005[...]

LED	Zustand		Bedeutung
Info2	Grün	Ein	Konfigurierte VPN-Verbindungen an Ausgang O1 sind aufgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze sind eingeschaltet
		Blinkt	Konfigurierte VPN-Verbindungen an Ausgang O1 werden auf- oder abgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze werden ein- oder ausgeschaltet
Info1	Grün	Ein	Konfigurierte VPN-Verbindungen an Ausgang O2 sind aufgebaut oder die an Ausgang O2 definierten Firewall-Regelsätze sind eingeschaltet
		Blinkt	Konfigurierte VPN-Verbindungen an Ausgang O2 werden auf- oder abgebaut oder die an Ausgang O2 definierten Firewall-Regelsätze werden ein- oder ausgeschaltet
WAN 1	Grün	Ein	Die LEDs befinden sich in den Buchsen (10/100 und Duplex-Anzeige) **Ethernet-Status**. Die LEDs zeigen den Status des entsprechenden Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN, WAN oder DMZ besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
DMZ1[1]	Grün	Ein	
LAN 1–4/5[2]	Grün	Ein	

[1] nur FL MGUARD RS4004

[2] nur FL MGUARD RS2005

3.2 Inbetriebnahme

3.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Gerätes nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Gerätes verbunden werden.

Für den Anschluss eines Modems oder eines seriellen Terminals an der RS-232-Schnittstelle benötigen Sie ein Nullmodem-Kabel, dessen Länge 10 m nicht überschreiten darf.

ACHTUNG: Gefahr von Sachschäden durch Störaussendungen

Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

ACHTUNG: Elektrostatische Entladung!

Beachten Sie beim Umgang mit dem Gerät die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) nach EN 61340-5-1 und IEC 61340-5-1.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

– Umgebungstemperatur:
  -20°C ... +60°C
– Maximale Luftfeuchtigkeit, nicht kondensierend:
  5 % ... 95 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

3.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

– Das Gerät
– Packungsbeilage
– Steckbare Schraubklemmen für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

3.2.3 mGuard-Firmware

Das Gerät muss mit mGuard-Firmware ab Version 8.1.5 betrieben werden.

3.3 FL MGUARD RS4004/RS2005 installieren

3.3.1 Montage/Demontage

ACHTUNG: Gerätebeschädigung
Montieren und demontieren Sie die Geräte nur im spannungsfreien Zustand

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

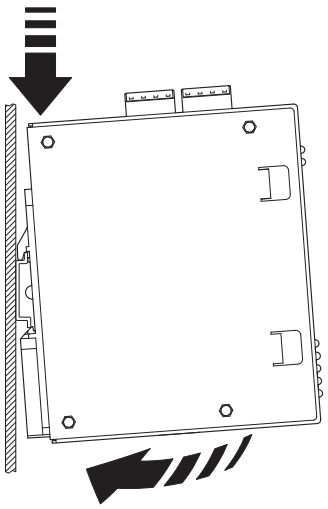


Bild 3-3 Montage des Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein. Drücken Sie das Gerät dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

3.3.2 Netzwerkverbindung anschließen

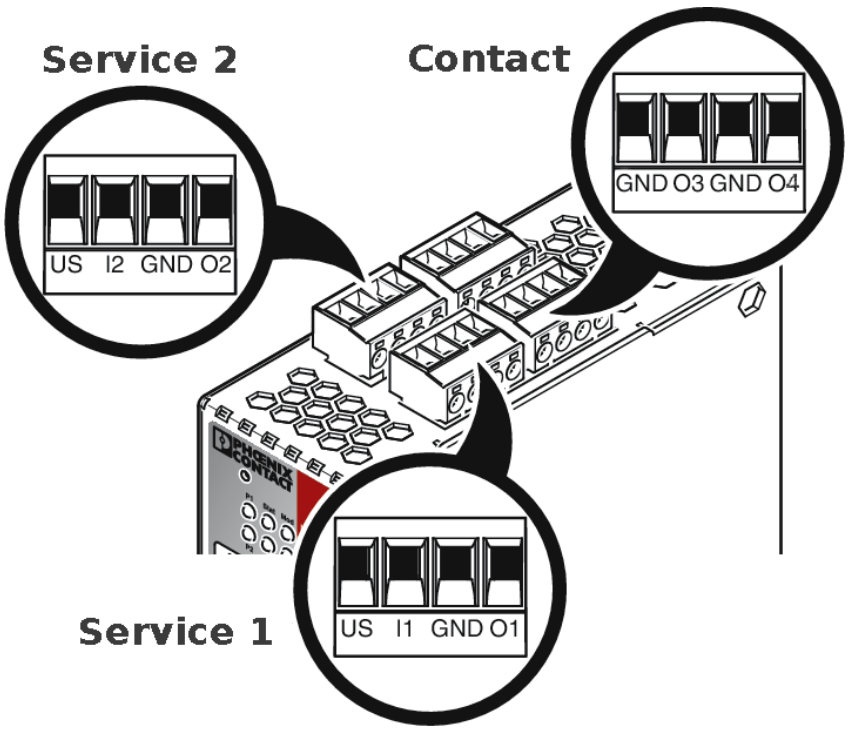
ACHTUNG: Sachschaden durch falsche Beschaltung
Schließen Sie die Netzwerk-Ports des Gerätes nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Gerätes verbunden werden.

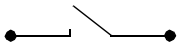
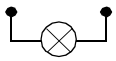
- Verbinden Sie das Gerät mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

3.3.3 Servicekontakte anschließen

ACHTUNG: Schließen Sie die Spannungs- und Masseausgänge **US** (bzw. **CMD V+**) und **GND nicht** an eine externe Spannungsquelle an.

Die steckbaren Schraubklemmen der Servicekontakte können während des Betriebs des Geräts entfernt oder aufgesetzt werden.



Service 1 + 2	US	I1/I2	GND	O1/O2
	Spannungs-ausgang (+) Versorgungs-spannung	Schalt-eingang 11...36 V DC	Masseaus-gang (-) Versorgungs-spannung	Kurz-schlussfes-ter Schal-tausgang [1]
	Beispiel 		Beispiel 	

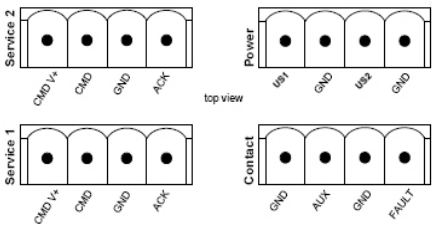
Power	24V	0V	24V	0V
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 3.3.4		nur beim FL MGUARD RS4004 siehe Kapitel 3.3.4	

Contact	GND	O3	GND	O4
	nicht ver-wendet	nicht ver-wendet	Meldeaus-gang (-)	Meldeaus-gang (+)[2]

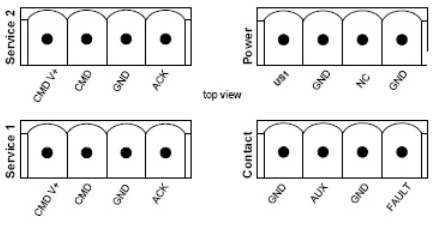
[1] Maximal 250 mA bei 11 ... 36 V DC

[2] 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

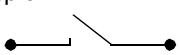
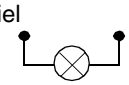
Die nachfolgend beschriebene Bezeichnung der Kontakte ist ebenfalls möglich:



FL MGUARD RS4004



FL MGUARD RS2005

Service 1 + 2	CMD V+	CMD	GND	ACK
	Spannungs-ausgang (+) Versorgungs-spannung	Schalt-eingang 11...36 V DC	Masseaus-gang (-) Versorgungs-spannung	Kurz-schlussfes-ter Schal-tausgang [1]
	Beispiel 		Beispiel 	

Power	US1	GND	US2	GND
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 3.3.4		nur beim FL MGUARD RS4004 siehe Kapitel 3.3.4	

Contact	GND	AUX	GND	FAULT
	nicht ver-wendet	nicht ver-wendet	Meldeaus-gang (-)	Meldeaus-gang (+)[2]

[1] Maximal 250 mA bei 11 ... 36 V DC

[2] 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Zwischen die **Servicekontakte US** und **I** (bzw. CMD V+ und CMD) kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Die Kontakte **O1/O2 (+)** und **O4 (+)** (bzw. ACK und FAULT) sind potenzialbehaftet, dauerkurzschlussfest und liefern jeweils maximal 250 mA.

Die Schalteingänge und Schaltausgänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen von SPS-Steuerungen. Achten Sie in diesem Fall auf ein gleiches Potenzial und die Spannungs- und Stromangaben.

Die Servicekontakte können je nach verwendeter Firmware-Version für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

3.3.4 Versorgungsspannung anschließen

WARNUNG: Das Gerät ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach IEC 60950/EN 60950/VDE 0805 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über eine steckbare Schraubklemme, die sich oben auf dem Gerät befindet.

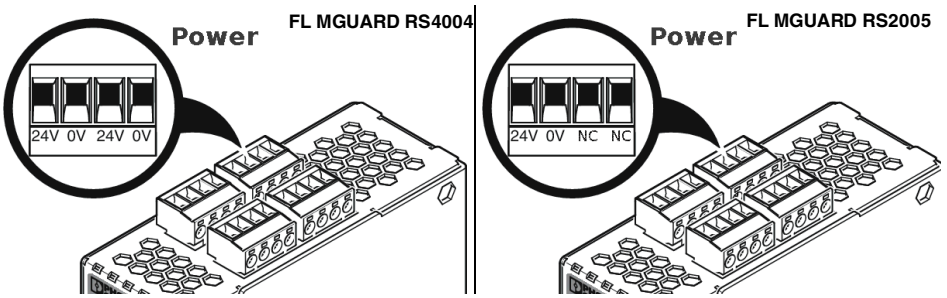


Bild 3-4 Versorgungsspannung anschließen

Anstatt der Bezeichnung **24V/24V** wird die Bezeichnung **US1/US2** ebenfalls verwendet.

Der **FL MGUARD RS4004** hat eine redundante Versorgungsspannung. Wenn Sie nur eine Versorgungsspannung anschließen, erhalten Sie eine Fehlermeldung.

- Nehmen Sie die steckbaren Schraubklemmen für Stromversorgung und Servicekontakte ab.
- Schließen Sie die Servicekontakte nicht an eine externe Spannungsquelle an.
- Verdrahten Sie die Versorgungsspannungsleitungen mit der entsprechenden Schraubklemme **24V/24V** (bzw. US1/US2) des Geräts. Ziehen Sie die Schrauben der Schraubklemmen mit 0,5 ... 0,8 Nm an.
- Stecken Sie die Schraubklemmen auf die vorgesehenen Buchsen auf der Oberseite des Geräts (siehe Bild 3-4).

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist. Beim FL MGUARD RS4004 leuchtet zusätzlich die Status-Anzeige P2 bei redundantem Anschluss der Versorgungsspannung.

Das Gerät bootet die Firmware. Die Status-Anzeige STAT blinkt grün. Das Gerät ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die Status-Anzeigen P1/P2 grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

Redundante Spannungsversorgung (FL MGUARD RS4004)

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den FL MGUARD RS4004 alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der FL MGUARD RS4004 über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge **24V/24V** (bzw. US1/US2) zuführen oder eine geeignete Drahtbrücke zwischen den Anschlüssen **24V und 24V** (bzw. US1 und US2) anbringen.

3.4 Konfiguration vorbereiten

3.4.1 Anschlussvoraussetzungen

– Das Gerät muss an mindestens einem aktiven Netzteil angeschlossen sein.
– **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
– **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass es eine Fernkonfiguration zulässt.
– Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

3.5 Konfiguration im Router-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter folgender IP-Adresse erreichbar:

– https://192.168.1.1/ (siehe Seite 50)

Alternativ kann per BootP eine IP-Adresse zugewiesen werden (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 51).

3.5.1 IP-Adresse 192.168.1.1

Im Router-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.

– Das Gerät ist im Auslieferungszustand.
– Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
– Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

3.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter der folgenden Adresse erreichbar:

Tabelle 3-3 Voreingestellte Adresse

Werkseinstellung	Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
FL MGUARD RS2005	Router	https://192.168.1.1/
FL MGUARD RS4004	Router	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des Geräts vollständig ein (siehe Tabelle 3-3).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 55).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.
  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.
  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 3-5 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

3.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Im Auslieferungszustand ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

3.8 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

3.9 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

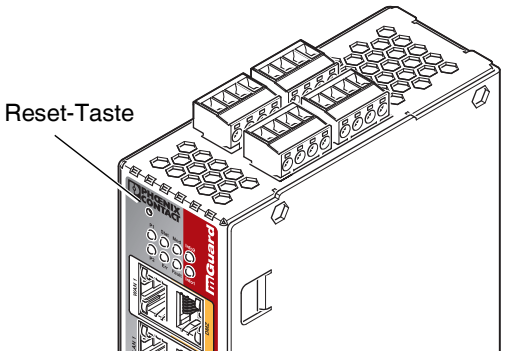


Bild 3-6 Reset-Taste

3.9.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED Err leuchtet
  (Alternativ können Sie die Spannungsversorgung unterbrechen und wieder anschließen.)

3.9.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 3-4 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Das Gerät wird in den Router-Modus mit fester IP-Adresse zurückgesetzt.

- Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
- Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
- Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

- Das Gerät befindet sich im Router- oder PPPoE-Modus.
- Die Geräteadresse des Geräts ist konfiguriert worden und Ihnen unbekannt.
- Sie kennen die aktuelle IP-Adresse des Geräts nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 3-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED Stat grün.
- Wenn die LED Stat grün erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED Stat grün
  Bei Misserfolg leuchtet die LED Err rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Router-Modus. Dann ist das Gerät wieder unter der entsprechenden Adresse zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

3.9.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

– **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

– alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
– diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

– Sie haben die Firmware des mGuard-Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
– Diese SD-Karte ist im Gerät eingesetzt.
– Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen in diesen Ordnern liegen:

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

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs Stat, Mod und Sig grün leuchten. Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware.Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED Stat blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs Stat, Mod und Sig bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche Betriebssystem und ist elektronisch signiert. Nur vom Hersteller signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED Stat leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, blinken die LEDs Stat, Mod und Sig gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren das mGuard-Gerät neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 51).

3.10 Technische Daten

Hardware-Eigenschaften	FL MGUARD RS4004	FL MGUARD RS2005
Plattform	Freescale Netzwerkprozessor	Freescale Netzwerkprozessor
Netzwerk-Schnittstellen	4 LAN-Ports (managed) I 1 DMZ-Port I 1 WAN-Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX	5 LAN-Ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	Seriell RS-232 I D-SUB 9-Stecker je 3 digitale Ein- und Ausgänge	Seriell RS-232 I D-SUB 9-Stecker je 3 digitale Ein- und Ausgänge
Speicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher
Redundanz-Optionen	optional: VPN I Router und Firewall	–
Stromversorgung	Spannungsbereich 11 ... 36 V DC, redundant	Spannungsbereich 11 ... 36 V DC
Stromaufnahme	typisch < 200 mA (24 V DC) maximal < 800 mA (10 V DC)	typisch < 200 mA (24 V DC) maximal < 800 mA (10 V DC)
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20	IP20
Temperaturbereich	-20 °C ... +60 °C (Betrieb) -20 °C ... +70 °C (Lagerung)	-20 °C ... +60 °C (Betrieb) -20 °C ... +70 °C (Lagerung)
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	749 g (TX/DTX)	749 g (TX)
Gewicht (inkl. Verpackung)	906 g (TX/DTX)	906 g (TX)

Firmware und Leistungswerte	FL MGUARD RS4004	FL MGUARD RS2005
Firmware-Kompatibilität	Firmware 8.1, Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt	
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.	
Virtual Private Network (VPN)	IPsec (IETF-Standard) optional bis zu 250 VPN-Tunnel	IPsec (IETF-Standard) bis zu 2 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 20 MBit/s Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.	
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software	
Diagnose	13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signalstatus, SIM-Status) I Service I/O I Log-File I Remote-Syslog	

Sonstiges	FL MGUARD RS4004	FL MGUARD RS2005
Besonderheiten	Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Secure Cloud ready	

4 TC MGUARD RS4000/RS2000 3G

Tabelle 4-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
TC MGUARD RS4000 3G VPN	2903440
TC MGUARD RS2000 3G VPN	2903441

Produktbeschreibung

Der **TC MGUARD RS4000 3G** eignet sich für die dezentrale Absicherung von Produktionszellen oder einzelnen Maschinen gegen Manipulationen.

Er verfügt über einen 4-Port managed LAN-Switch und ein industrielles 3G-Mobilfunk-Modem für GPRS-, UMTS- und CDMA-Netze mit einer Geschwindigkeit von bis zu 14,4 MBit/s im Download.

Die Mobilfunk-Schnittstelle kann u. a. als Wegeredundanz zur WAN-Schnittstelle geschaltet werden. Ein dedizierter DMZ-Port mit eigenen Firewall-Regeln ermöglicht eine Segmentierung und differenziertere Sicherheitskonzepte. Der GPS- /GLONASS-Empfänger ermöglicht eine Zeitsynchronisation und Ortungsdienste. Sie können Automatisierungsgeräte mit seriellen Schnittstellen in Netzwerke einbinden, da ein COM-Server integriert ist.

Für eine softwareunabhängige Fernwartung kann der TC MGUARD RS4000 3G als VPN-Router für bis zu 10 (optional bis zu 250) parallele, IPsec-verschlüsselte VPN-Tunnel eingesetzt werden.

Der **TC MGUARD RS2000 3G** ist eine Variante mit einfacher Firewall und kann als VPN-Client für bis zu zwei parallele, IPsec-verschlüsselte VPN-Tunnel eingesetzt werden. Er eignet sich für sichere Fernwartungsszenarien an Orten ohne kabelgebundenes Netzwerk und ermöglicht die Anbindung weltweit verteilter Maschinen und Steuerungen.

Beide Varianten unterstützen einen auswechselbaren Konfigurationsspeicher in Form einer SD-Karte. Zur Erhöhung der Sicherheit können VPN-Verbindungen per Schaltkontakt, SMS oder Software-Schnittstelle ein- bzw. ausgeschaltet werden. Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

Bild 4-1 TC MGUARD RS2000 3G/TC MGUARD RS4000 3G

4.1 Bedienelemente und Anzeigen

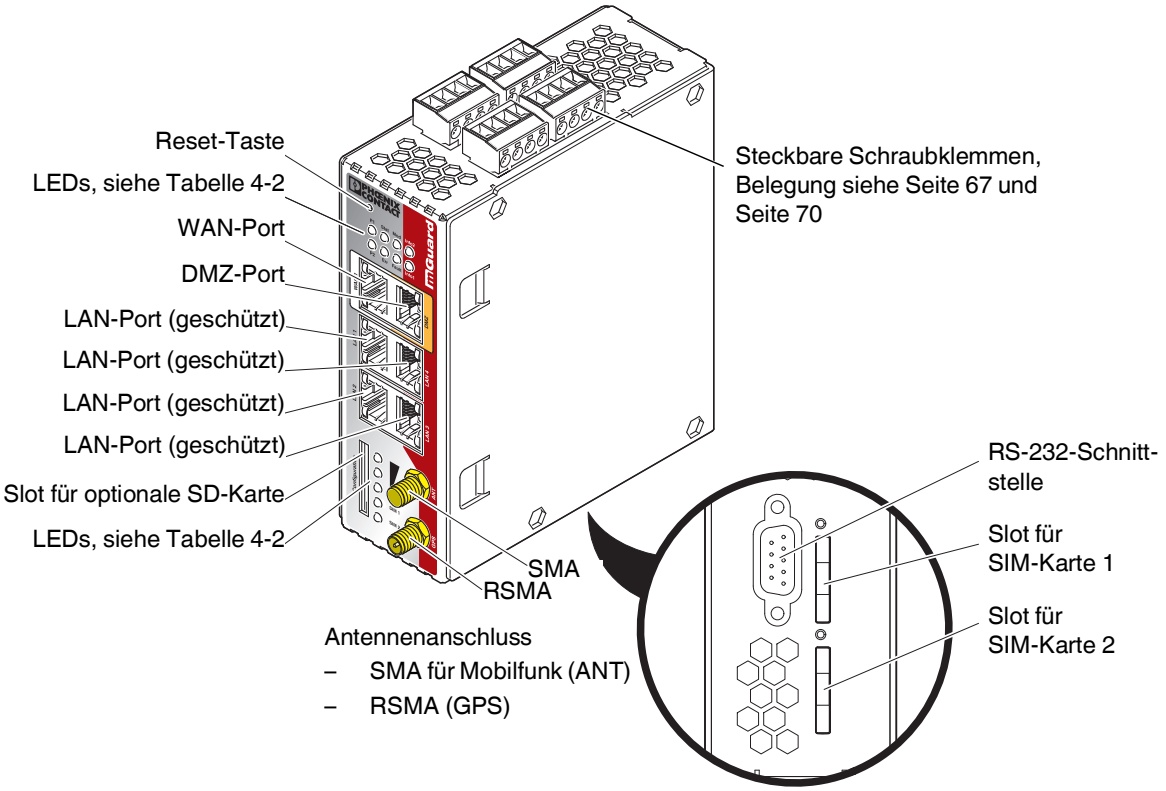


Bild 4-2 Bedienelemente und Anzeigen des TC MGUARD RS4000 3G

Tabelle 4-2 Anzeigen des TC MGUARD RS4000 3G und TC MGUARD RS2000 3G

LED	Zustand		Bedeutung
P1	Grün	Ein	Stromversorgung 1 ist aktiv
P2	Grün	Ein	Stromversorgung 2 ist aktiv (TC MGUARD RS2000 3G: unbelegt)
Stat	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
Err	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Reset-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe Seite 77) oder wenden Sie sich an Ihren Händler.
Stat + Err	Abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
Mod	Grün	Ein	Verbindung per Modem hergestellt
Fault	Rot	Ein	Der Meldeausgang nimmt aufgrund eines Fehlers Low-Pegel ein (invertierte Logik). Während eines Neustarts ist der Meldeausgang inaktiv.

Tabelle 4-2 Anzeigen des TC MGUARD RS4000 3G und TC MGUARD RS2000 3G [...]

LED	Zustand		Bedeutung			
Info2	Grün	Ein	Bis Firmware-Version 8.0		Ab Firmware-Version 8.1	
			Konfigurierte VPN-Verbindung an Ausgang O1 ist aufgebaut		Konfigurierte VPN-Verbindungen an Ausgang O1 sind aufgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze sind eingeschaltet	
		Blinkt	Konfigurierte VPN-Verbindung an Ausgang O1 wird auf- oder abgebaut		Konfigurierte VPN-Verbindungen an Ausgang O1 werden auf- oder abgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze werden ein- oder ausgeschaltet	
Info1	Grün	Ein	Bis Firmware-Version 8.0		Ab Firmware-Version 8.1	
			Konfigurierte VPN-Verbindung an Ausgang O2 ist aufgebaut		Konfigurierte VPN-Verbindungen an Ausgang O2 sind aufgebaut oder die an Ausgang O2 definierten Firewall-Regelsätze sind eingeschaltet	
		Blinkt	Konfigurierte VPN-Verbindung an Ausgang O2 wird auf- oder abgebaut		Konfigurierte VPN-Verbindungen an Ausgang O2 werden auf- oder abgebaut oder die an Ausgang O2 definierten Firewall-Regelsätze werden ein- oder ausgeschaltet	
WAN 1*	Grün	Ein	Die LEDs befinden sich in den Buchsen (10/100 und Duplex-Anzeige)			
DMZ*	Grün	Ein	**Ethernet-Status**. Die LEDs zeigen den Status des entsprechenden Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN, WAN oder DMZ besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.			
LAN 1–4	Grün	Ein				
Bargraph	LED 3	Oben	Aus	Aus	Aus	Grün
	LED 2	Mitte	Aus	Aus	Grün	Grün
	LED 1	Unten	Aus	Gelb	Gelb	Gelb
	Signalstärke		-113 ... 111 dBm	-109 ... 89 dBm	-87 ... 67 dBm	-65 ... 51 dBm
	Netzempfang		Sehr schlecht bis kein	Ausreichend	Gut	Sehr gut
SIM 1	Grün	Ein	SIM-Karte 1 aktiv			
		Blinkt	Keine oder falsche PIN eingegeben			
SIM 2	Grün	Ein	SIM-Karte 2 aktiv			
		Blinkt	Keine oder falsche PIN eingegeben			

* nur TC MGUARD RS4000 3G

4.2 Inbetriebnahme

4.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Für den Anschluss eines Modems oder eines seriellen Terminals an der RS-232-Schnittstelle benötigen Sie ein Nullmodem-Kabel, dessen Länge 10 m nicht überschreiten darf.

ACHTUNG: Gefahr von Sachschäden durch Störaussendungen

Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

ACHTUNG: Elektrostatische Entladung!

Beachten Sie beim Umgang mit dem Gerät die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) nach EN 61340-5-1 und IEC 61340-5-1.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

– Umgebungstemperatur: -40°C ... +60°C
– Maximale Luftfeuchtigkeit, nicht kondensierend: 5 % ... 95 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Verlängerte Hochlaufzeit bei niedrigen Temperaturen

Niedrige Temperaturen führen zu einer verlängerten Hochlaufzeit des Geräts. Die Betriebsbereitschaft wird nach maximal 5 Minuten erreicht.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

4.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

– Das Gerät
– Packungsbeilage
– Steckbare Schraubklemmen für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

4.2.3 mGuard-Firmware

– Das Gerät muss mit mGuard-Firmware ab Version 8.0 betrieben werden.

4.3 TC MGUARD RS4000/RS2000 3G installieren

4.3.1 Montage/Demontage

ACHTUNG: Gerätebeschädigung
Montieren und demontieren Sie die Geräte nur im spannungsfreien Zustand

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

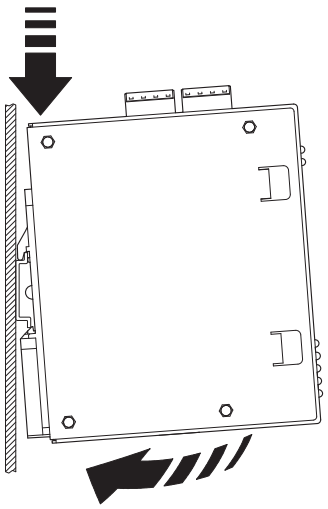


Bild 4-3 Montage des Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein und drücken Sie das Gerät dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

4.3.2 Netzwerkverbindung anschließen

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

- Verbinden Sie das Gerät mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört. Verwenden Sie UTP-Leitungen mit einer Impedanz von 100 Ω.
- Verbinden Sie die interne Netzwerkschnittstelle LAN des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

4.3.3 Servicekontakte anschließen

ACHTUNG: Schließen Sie die Spannungs- und Masseausgänge **nicht** an eine externe Spannungsquelle an.

Die steckbaren Schraubklemmen der Servicekontakte können während des Betriebs des Geräts entfernt oder aufgesetzt werden.

Der TC MGUARD RS4000/RS2000 3G hat jeweils drei digitale Ein- und Ausgänge. Diese werden in der Web-Oberfläche konfiguriert, z. B. als Steuersignal zum Starten und Stoppen von VPN-Verbindungen.

Die digitalen Ein- und Ausgänge werden wie folgt angeschlossen.

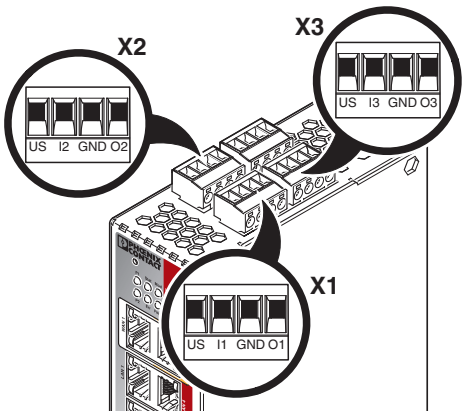
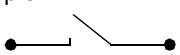
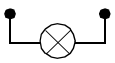


Bild 4-4 Servicekontakte

	Steuerungsschalter CMD		Meldeausgang (digital) ACK	
	US	**I1, I2, I3**	**GND**	**O1, O2, O3**
X1 ... X3	Spannungsausgang (+) Versorgungsspannung	Schalteingang 11 ... 36 V DC	Masseausgang (-) Versorgungsspannung	Kurzschlussfester Schaltausgang, maximal 250 mA bei 11 ... 36 V DC
	Beispiel 		Beispiel 	

Zwischen die **Servicekontakte US und I** kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Die **Kontakte O1–3** sind potenzialbehaftet, dauerkurzschlussfest und liefern jeweils maximal 250 mA.

Die Schalteingänge und Schaltausgänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen einer SPS. Achten Sie in diesem Fall auf ein gleiches Potenzial und die Spannungs- und Stromangaben.

Die Servicekontakte können je nach verwendeter Firmware-Version für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

4.3.4 Antennen

Um eine Mobilfunk-Verbindung aufzubauen, muss eine passende **Antenne** an die Geräte angeschlossen werden.

ACHTUNG: Gesundheitsgefahr durch Antennenstrahlung

Im normalen Betrieb muss ein Abstand von mindestens 20 cm zwischen anwesenden Personen und der Antenne eingehalten werden.

ACHTUNG: Erlöschen der Betriebserlaubnis

Der Betrieb des Funksystems ist nur unter Verwendung des bei Phoenix Contact erhältlichen Zubehörs zulässig. Der Einsatz von anderen Zubehörkomponenten kann zum Erlöschen der Betriebsgenehmigung führen.

Das zugelassene Zubehör für dieses Funksystem finden Sie am Produkt unter folgender Internet-Adresse: phoenixcontact.net/products.

Wir empfehlen die kombinierte Mobilfunk-GPS-Antenne mit Rundstrahlcharakteristik, Antennenkabel mit SMA-Rundstecker (GSM/UMTS) und R-SMA-Rundstecker (TC ANT MOBILE/GPS, 2903590 von Phoenix Contact).

Beim **TC MGUARD RS2000 3G** steht das WAN nur über den Mobilfunk zur Verfügung, da keine WAN-Schnittstelle vorhanden ist. Die Mobilfunk-Funktion ist voreingestellt.
TC MGUARD RS2000 3G kann nur im Router-Modus betrieben werden.

Antennen anschließen

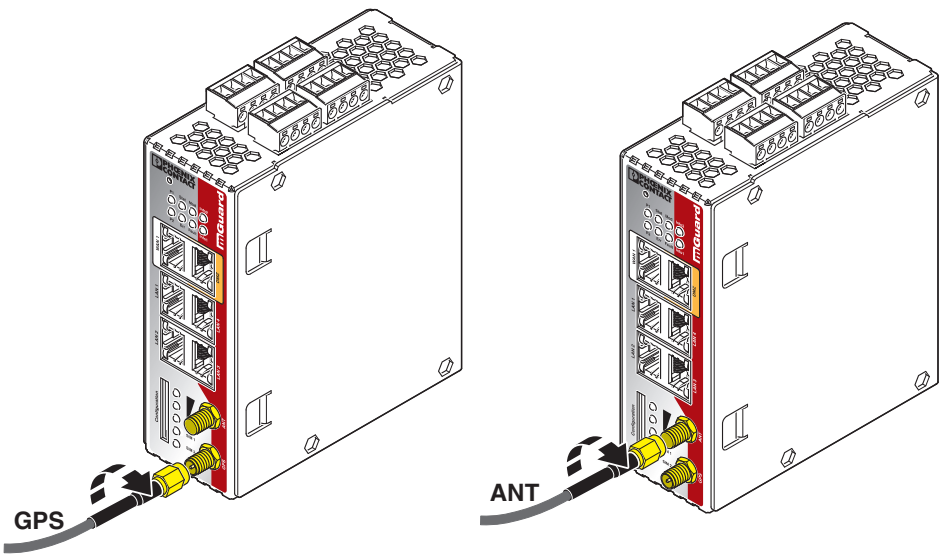


Bild 4-5 Antennenanschluss

- Schließen Sie eine bzw. zwei geeignete Antenne an den Antennenanschluss an.
  Antennenanschluss
  - SMA für Mobilfunk (ANT)
  - RSMA (GPS)
- Wenn der Bargraph einen guten oder sehr guten Empfang anzeigt, fixieren Sie die Antenne (siehe „Bargraph“ auf Seite 63).

4.3.5 SIM-Karte

Um eine Mobilfunk-Verbindung aufzubauen, benötigt das Gerät mindestens eine gültige **Mini-SIM-Karte** im ID-000-Format, über die er sich einem Mobilfunknetz zuordnet und authentifiziert.

Das Gerät kann mit zwei SIM-Karten ausgestattet werden. Die SIM-Karte in Schacht SIM 1 ist die primäre SIM-Karte, über die in der Regel die Verbindung aufgebaut wird. Wenn diese Verbindung ausfällt, kann optional auf die zweite SIM-Karte in Schacht SIM 2 zurückgegriffen werden. Sie können einstellen, ob und unter welchen Bedingungen die Verbindung dann wieder auf die primäre SIM-Karte zurückgestellt wird.

Der Zustand der SIM-Karten wir über zwei LEDs an der Front angezeigt. Die LEDs SIM1 und SIM2 leuchten grün, wenn die SIM-Karte aktiv ist. Wenn keine PIN eingegeben wurde, blinkt die LED grün.

Qualität der Mobilfunk-Verbindung

Die Signalstärke der Mobilfunk-Verbindung wird über drei LEDs an der Front des Geräts angezeigt. Die LEDs funktionieren als Bargraph (siehe „Bargraph“ auf Seite 63).

Für eine stabile Datenübertragung empfehlen wir mindestens einen guten Netzempfang. Bei nur ausreichendem Netzempfang können nur SMS-Nachrichten versendet und empfangen werden.

SIM-Karte einlegen

Vom Mobilfunkanbieter (Provider) erhalten Sie eine SIM-Karte, auf der alle Daten und Services Ihres Anschlusses gespeichert sind. Wenn Sie in den USA CDMA-Netze (z. B. von Verizon Wireless) nutzen, erhalten Sie keine SIM. Stellen Sie das Gerät über die Web-Oberfläche auf einen CDMA-Provider um.

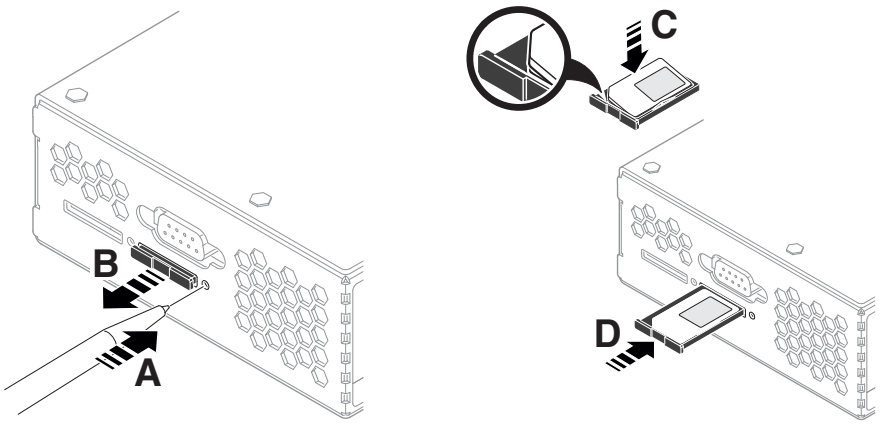


Bild 4-6 SIM-Karte einlegen

Zum Einsetzen der SIM-Karte gehen Sie wie folgt vor:

- Drücken Sie auf den Entriegelungsknopf.
- Entnehmen Sie den SIM-Karten-Halter.
- Legen Sie die SIM-Karte so ein, dass der SIM-Chip sichtbar bleibt.
- Stecken Sie den SIM-Karten-Halter mit der SIM-Karte vollständig in das Gerät, bis dieser bündig mit dem Gehäuse abschließt.

4.3.6 Versorgungsspannung anschließen

WARNUNG: Da Gerät ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach IEC 60950/EN 60950/VDE 0805 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über eine steckbare Schraubklemme, die sich oben auf dem Gerät befindet.

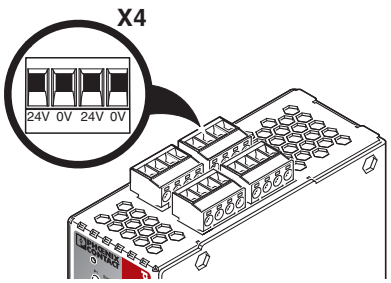
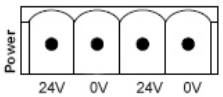
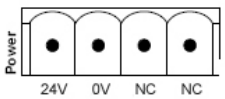


Bild 4-7 Versorgungsspannung anschließen (TC MGUARD RS4000 3G)

Tabelle 4-3 Versorgungsspannung des Geräts

TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
	

Der TC MGUARD RS4000 3G hat eine redundante Versorgungsspannung. Wenn Sie nur eine Versorgungsspannung anschließen, erhalten Sie eine Fehlermeldung.

- Nehmen Sie die steckbaren Schraubklemmen für Stromversorgung und Servicekontakte ab.
- Verdrahten Sie die Versorgungsspannungsleitungen der Schraubklemme X4 des Geräts. Ziehen Sie die Schrauben der Schraubklemmen mit 0,5 ... 0,8 Nm an.
- Stecken Sie die Steckbare Schraubklemme auf die vorgesehenen Buchsen auf der Oberseite des Geräts.

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist. Beim TC MGUARD RS4000 3G leuchtet zusätzlich die Status-Anzeige P2 bei redundantem Anschluss der Versorgungsspannung.

Das Gerät bootet die Firmware. Die LED STAT blinkt grün. Das Gerät ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die LEDs P1/P2 grün und die LED STAT blinkt grün im Heartbeat.

Redundante Spannungsversorgung (TC MGUARD RS4000 3G)

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den TC MGUARD RS4000 3G alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der TC MGUARD RS4000 3G über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder eine geeignete Drahtbrücke zwischen den Anschlüssen anbringen.

4.4 Konfiguration vorbereiten

4.4.1 Anschlussvoraussetzungen

– Das Gerät muss an mindestens einem aktiven Netzteil angeschlossen sein.
– **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
– **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
– Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

4.5 Konfiguration im Router-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter folgender IP-Adresse erreichbar:
– https://192.168.1.1/

4.5.1 IP-Adresse 192.168.1.1

Im Router-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.
– Das Gerät ist im Auslieferungszustand.
– Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
– Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:
- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard -Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

4.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter der folgenden Adresse erreichbar:

Tabelle 4-4 Voreingestellte Adresse

Werkseinstellung	Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
TC MGUARD RS4000 3G	Router	https://192.168.1.1/
TC MGUARD RS2000 3G	Router	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die IP-Adresse des Geräts vollständig ein (siehe Tabelle 4-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die IP-Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 77).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.
  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.
  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 4-8 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

4.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

4.8 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

4.9 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

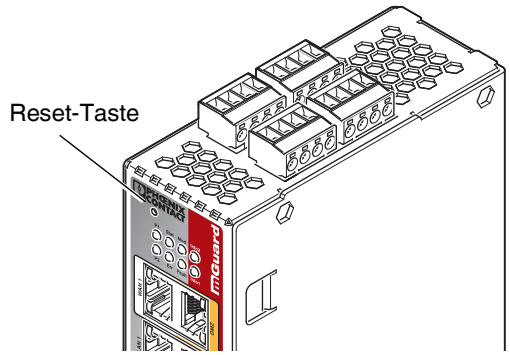


Bild 4-9 Reset-Taste

4.9.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED Err leuchtet (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

4.9.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 4-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Das Gerät wird in den Router-Modus mit fester IP-Adresse zurückgesetzt.

- Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
- Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
- Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

- Das Gerät befindet sich im Router- oder PPPoE-Modus.
- Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
- Sie kennen die aktuelle IP-Adresse des Geräts nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 4-6 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED Stat grün.
- Wenn die LED Stat grün erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED Stat grün
  Bei Misserfolg leuchtet die LED Err rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Router-Modus. Dann ist das Gerät wieder unter der entsprechenden Adresse zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

4.9.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

– **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

– alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
– diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

– Sie haben die mGuard-Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
– Diese SD-Karte ist im mGuard eingesetzt.
– Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:

  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s
  Firmware/pxs8_03001_0100617.usf.xz.p7s

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs Stat, Mod und Sig grün leuchten. Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware.Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED Stat blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs Stat, Mod und Sig bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED Stat leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, blinken die LEDs Stat, Mod und Sig gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie das mGuard-Gerät neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 73).

4.10 Technische Daten

Hardware-Eigenschaften	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Plattform	Freescale Netzwerkprozessor	Freescale Netzwerkprozessor
Netzwerk-Schnittstellen	4 LAN-Ports (managed) I 1 DMZ-Port I 1 WAN-Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX	4 LAN-Ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX
Funk-Schnittstelle	WAN I GSM I GPRS I EDGE I UMTS I CDMA2000	WAN I GSM I GPRS I EDGE I UMTS I CDMA2000
SIM-Schnittstellen (1 + 2)	1,8 V I 3 V, redundant	1,8 V I 3 V, redundant
Sonstige Schnittstellen	Seriell RS-232 I D-SUB 9-Stecker je 3 digitale Ein- und Ausgänge	Seriell RS-232 I D-SUB 9-Stecker je 3 digitale Ein- und Ausgänge
Speicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher
Redundanz-Optionen	optional: VPN I Router und Firewall	–
Stromversorgung	Spannungsbereich 11 ... 36 V DC, redundant	Spannungsbereich 11 ... 36 V DC
Leistungsaufnahme	typisch < 200 mA (24 V DC) maximal < 800 mA (10 V DC)	typisch < 200 mA (24 V DC) maximal < 800 mA (10 V DC)
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20	IP20
Temperaturbereich	-40 °C ... +60 °C (Betrieb) -40 °C ... +70 °C (Lagerung)	-40 °C ... +60 °C (Betrieb) -40 °C ... +70 °C (Lagerung)
Vibrationsfestigkeit nach EN 60068-2-6/IEC 60068-2-6	5g, 150 Hz, 2,5 h, in XYZ-Richtung	5g, 150 Hz, 2,5 h, in XYZ-Richtung
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	850 g	835 g

Firmware und Leistungswerte	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Firmware-Kompatibilität	mGuard v8.0 oder höher; Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt	
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 110 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.	
Virtual Private Network (VPN)	IPsec (IETF-Standard) optional bis zu 250 VPN-Tunnel	IPsec (IETF-Standard) bis zu 2 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 20 MBit/s Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.	
Datenrate (Mobilfunk)	Abhängig von der Mobilfunkverbindung ≤ 5,7 Mbit/s (HSDPA) im Upload ≤ 14,4 Mbit/s (HSDPA) im Download	
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software	
Diagnose	13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signalstatus, SIM-Status) I Service I/OI Log-File I Remote-Syslog	

Störaussendung nach EN 61000-6-4	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Funkstörspannung nach EN 55011	EN 55011 Klasse A Einsatzgebiet Industrie	
Funkstörstrahlung nach EN 55011	EN 55011 Klasse A Einsatzgebiet Industrie	
Störaussendung	EN 61000-6-4	
Kriterium A	Normales Betriebsverhalten innerhalb der festgelegten Grenzen	
Kriterium B	Vorübergehende Beeinträchtigung des Betriebsverhaltens, die das Gerät selbst wieder korrigiert	

Sonstiges	TC MGUARD RS4000 3G	TC MGUARD RS2000 3G
Konformität	CE I FCC I UL 508 I Galvanische Trennung (VCC // PE) I ANSI / ISA 12.12 Class I Div. 2	
Besonderheiten	GPS/GLONASS-Empfänger I Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Secure Cloud ready	

5 TC MGUARD RS4000/RS2000 4G

Tabelle 5-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
TC MGUARD RS4000 4G VPN	2903586
TC MGUARD RS2000 4G VPN	2903588
TC MGUARD RS4000 4G VZW VPN	1010461 (Verizon Wireless – USA)
TC MGUARD RS2000 4G VZW VPN	1010462 (Verizon Wireless – USA)
TC MGUARD RS4000 4G ATT VPN	1010463 (AT&T – USA)
TC MGUARD RS2000 4G ATT VPN	1010464 (AT&T – USA)

Produktbeschreibung

Die vier für den US-amerikanischen Mark konzipierten Geräte-Varianten (**VZW** und **ATT**) können ausschließlich in den Mobilfunknetzen der Mobilfunkanbieter

– *Verizon Wireless* (TC MGUARD RS4000/RS2000 4G VZW VPN) bzw.
– *AT&T* (TC MGUARD RS4000/RS2000 4G ATT VPN) betrieben werden.

Bild 5-1 TC MGUARD RS4000 4G

Der **TC MGUARD RS4000 4G** eignet sich für die dezentrale Absicherung von Produktionszellen oder einzelnen Maschinen gegen Manipulationen. Er verfügt über einen 4-Port managed LAN-Switch und ein industrielles 4G-Mobilfunk-Modem für

– **TC MGUARD RS4000 4G VPN:** GPRS-, UMTS-, LTE- und CDMA-Netze
– **TC MGUARD RS4000 4G VZW VPN:** LTE-Netze
– **TC MGUARD RS4000 4G ATT VPN:** UMTS- und LTE-Netze

mit einer Geschwindigkeit von bis zu 150 MBit/s im Download.

Die Mobilfunk-Schnittstelle kann u. a. als Wegeredundanz zur WAN-Schnittstelle geschaltet werden. Ein dedizierter DMZ-Port mit eigenen Firewall-Regeln ermöglicht eine Segmentierung und differenziertere Sicherheitskonzepte. Der GPS- /GLONASS-Empfänger ermög-

licht eine Zeitsynchronisation und Ortungsdienste (nur die Geräte 2903586 und 2903588). Sie können Automatisierungsgeräte mit seriellen Schnittstellen in Netzwerke einbinden, da ein COM-Server integriert ist.

Für eine softwareunabhängige Fernwartung kann der TC MGUARD RS4000 4G als VPN-Router für bis zu 10 (optional bis zu 250) parallele, IPsec-verschlüsselte VPN-Tunnel eingesetzt werden.

Der **TC MGUARD RS2000 4G** ist eine Variante mit einfacher Firewall und kann als VPN-Client für bis zu zwei parallele, IPsec-verschlüsselte VPN-Tunnel eingesetzt werden. Er eignet sich für sichere Fernwartungsszenarien an Orten ohne kabelgebundenes Netzwerk und ermöglicht die Anbindung weltweit verteilter Maschinen und Steuerungen.

Unterstützte Mobilfunknetze:

- **TC MGUARD RS2000 4G VPN:** GPRS, UMTS, LTE und CDMA-Netze
- **TC MGUARD RS2000 4G VZW VPN:** LTE
- **TC MGUARD RS2000 4G ATT VPN:** UMTS, LTE

Beide Varianten unterstützen einen auswechselbaren Konfigurationsspeicher in Form einer SD-Karte. Zur Erhöhung der Sicherheit können VPN-Verbindungen per Schaltkontakt, SMS oder Software-Schnittstelle ein- bzw. ausgeschaltet werden. Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

5.1 Bedienelemente und Anzeigen

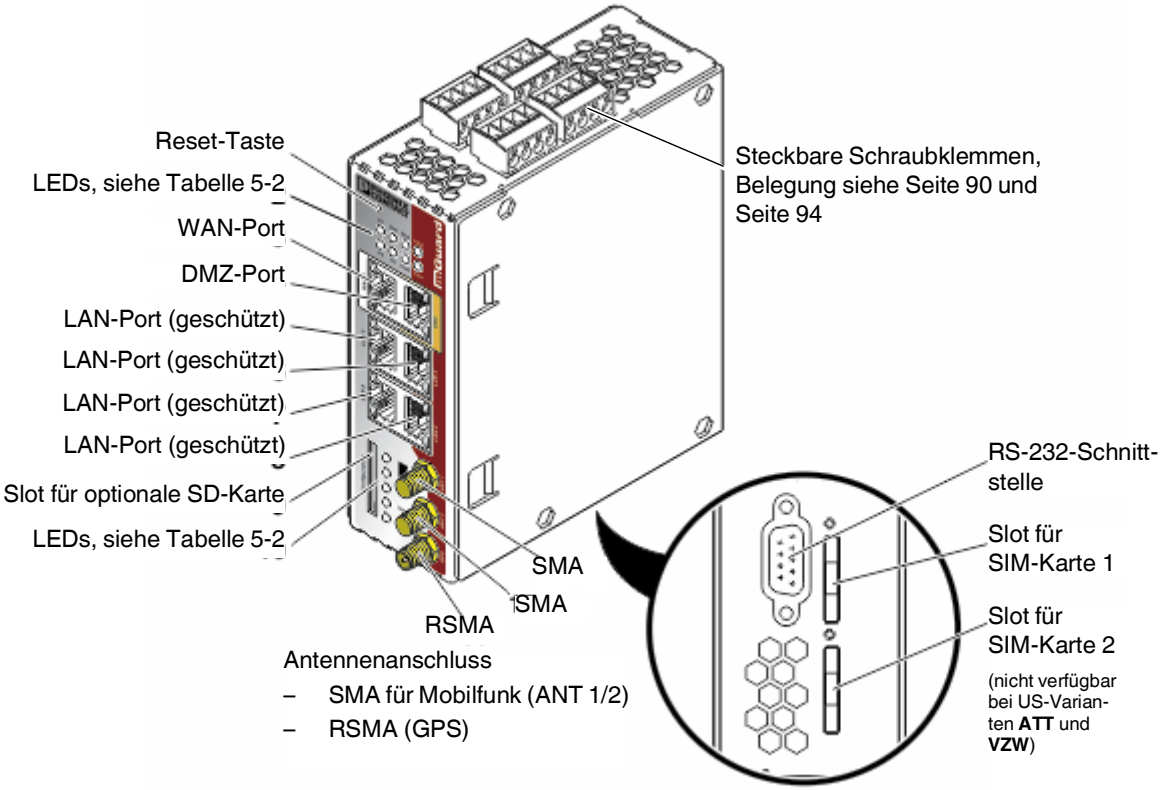


Bild 5-2 Bedienelemente und Anzeigen des TC MGUARD RS4000 4G

Tabelle 5-2 Anzeigen des TC MGUARD RS4000 4G und TC MGUARD RS2000 4G

LED	Zustand		Bedeutung
P1	Grün	Ein	Stromversorgung 1 ist aktiv
P2	Grün	Ein	Stromversorgung 2 ist aktiv (TC MGUARD RS2000 4G: unbelegt)
Stat	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
Err	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Reset-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe Seite 101) oder wenden Sie sich an Ihren Händler.
Stat + Err	Abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
Mod	Grün	Ein	Verbindung per Modem hergestellt
Fault	Rot	Ein	Der Meldeausgang nimmt aufgrund eines Fehlers Low-Pegel ein (invertierte Logik). Während eines Neustarts ist der Meldeausgang inaktiv.

Tabelle 5-2 Anzeigen des TC MGUARD RS4000 4G und TC MGUARD RS2000 4G [...]

LED	Zustand		Bedeutung			
Info2	Grün	Ein	Bis Firmware-Version 8.0		Ab Firmware-Version 8.1	
			Konfigurierte VPN-Verbindung an Ausgang O1 ist aufgebaut		Konfigurierte VPN-Verbindungen an Ausgang O1 sind aufgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze sind eingeschaltet	
		Blinkt	Konfigurierte VPN-Verbindung an Ausgang O1 wird auf- oder abgebaut		Konfigurierte VPN-Verbindungen an Ausgang O1 werden auf- oder abgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze werden ein- oder ausgeschaltet	
Info1	Grün	Ein	Bis Firmware-Version 8.0		Ab Firmware-Version 8.1	
			Konfigurierte VPN-Verbindung an Ausgang O2 ist aufgebaut		Konfigurierte VPN-Verbindungen an Ausgang O2 sind aufgebaut oder die an Ausgang O2 definierten Firewall-Regelsätze sind eingeschaltet	
		Blinkt	Konfigurierte VPN-Verbindung an Ausgang O2 wird auf- oder abgebaut		Konfigurierte VPN-Verbindungen an Ausgang O2 werden auf- oder abgebaut oder die an Ausgang O2 definierten Firewall-Regelsätze werden ein- oder ausgeschaltet	
WAN 1*	Grün	Ein	Die LEDs befinden sich in den Buchsen (10/100 und Duplex-Anzeige)			
DMZ*	Grün	Ein	**Ethernet-Status**. Die LEDs zeigen den Status des entsprechenden Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN, WAN oder DMZ besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.			
LAN 1–4	Grün	Ein				
Bargraph	LED 3	Oben	Aus	Aus	Aus	Grün
	LED 2	Mitte	Aus	Aus	Grün	Grün
	LED 1	Unten	Aus	Gelb	Gelb	Gelb
	Signalstärke		-113 ... 111 dBm	-109 ... 89 dBm	-87 ... 67 dBm	-65 ... 51 dBm
	Netzempfang		Sehr schlecht bis kein	Ausreichend	Gut	Sehr gut
SIM 1	Grün	Ein	SIM-Karte 1 aktiv			
		Blinkt	Keine oder falsche PIN eingegeben			
SIM 2 (nicht verfügbar bei US-Varianten **ATT** und **VZW**)	Grün	Ein	SIM-Karte 2 aktiv			
		Blinkt	Keine oder falsche PIN eingegeben			

* nur TC MGUARD RS4000 4G

5.2 Inbetriebnahme

5.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Für den Anschluss eines Modems oder eines seriellen Terminals an der RS-232-Schnittstelle benötigen Sie ein Nullmodem-Kabel, dessen Länge 10 m nicht überschreiten darf.

ACHTUNG: Gefahr von Sachschäden durch Störaussendungen

Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

ACHTUNG: Elektrostatische Entladung!

Beachten Sie beim Umgang mit dem Gerät die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) nach EN 61340-5-1 und IEC 61340-5-1.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

– Umgebungstemperatur: -40°C ... +60°C
– Maximale Luftfeuchtigkeit, nicht kondensierend: 5 % ... 95 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Verlängerte Hochlaufzeit bei niedrigen Temperaturen

Niedrige Temperaturen führen zu einer verlängerten Hochlaufzeit des Geräts. Die Betriebsbereitschaft wird nach maximal 5 Minuten erreicht.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

5.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

– Das Gerät
– Packungsbeilage
– Steckbare Schraubklemmen für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

5.2.3 mGuard-Firmware

– Die Geräte müssen mit mGuard-Firmware ab Version 8.4 () oder 8.7.0 () betrieben werden.

5.3 TC MGUARD RS4000/RS2000 4G installieren

5.3.1 Montage/Demontage

ACHTUNG: Gerätebeschädigung
Montieren und demontieren Sie die Geräte nur im spannungsfreien Zustand

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

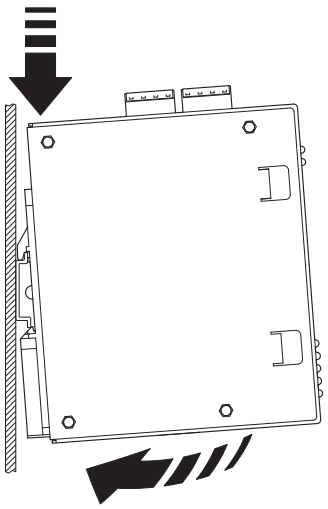


Bild 5-3 Montage des Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein und drücken Sie das Gerät dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

5.3.2 Netzwerkverbindung anschließen

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

- Verbinden Sie das Gerät mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört. Verwenden Sie UTP-Leitungen mit einer Impedanz von 100 Ω.
- Verbinden Sie die interne Netzwerkschnittstelle LAN des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

5.3.3 Servicekontakte anschließen

ACHTUNG: Schließen Sie die Spannungs- und Masseausgänge **nicht** an eine externe Spannungsquelle an.

Die steckbaren Schraubklemmen der Servicekontakte können während des Betriebs des Geräts entfernt oder aufgesetzt werden.

Der TC MGUARD RS4000/RS2000 4G hat jeweils drei digitale Ein- und Ausgänge. Diese werden in der Web-Oberfläche konfiguriert, z. B. als Steuersignal zum Starten und Stoppen von VPN-Verbindungen.

Die digitalen Ein- und Ausgänge werden wie folgt angeschlossen.

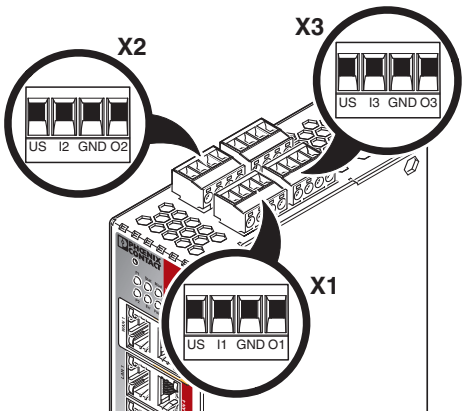
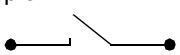
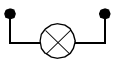


Bild 5-4 Servicekontakte

	Steuerungsschalter CMD		Meldeausgang (digital) ACK	
X1 ... X3	**US**	**I1, I2, I3**	**GND**	**O1, O2, O3**
	Spannungsausgang (+) Versorgungsspannung	Schalteingang 11 ... 36 V DC	Masseausgang (-) Versorgungsspannung	Kurzschlussfester Schaltausgang, maximal 250 mA bei 11 ... 36 V DC
	Beispiel 		Beispiel 	

Zwischen die **Servicekontakte US und I** kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Die **Kontakte O1–3** sind potenzialbehaftet, dauerkurzschlussfest und liefern jeweils maximal 250 mA.

Die Schalteingänge und Schaltausgänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen einer SPS. Achten Sie in diesem Fall auf ein gleiches Potenzial und die Spannungs- und Stromangaben.

Die Servicekontakte können je nach verwendeter Firmware-Version für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

5.3.4 Antennen

Um eine Mobilfunk-Verbindung aufzubauen, müssen passende **Antennen** an die Geräte angeschlossen werden.

TC MGUARD RS4000/RS2000 4G-Geräte haben zwei Mobilfunk-Antennenanschlüsse. Um einen optimalen LTE-Empfang zu erreichen, schließen Sie immer zwei Antennen an.

ACHTUNG: Gesundheitsgefahr durch Antennenstrahlung

Im normalen Betrieb muss ein Abstand von mindestens 20 cm zwischen anwesenden Personen und den Antennen eingehalten werden.

ACHTUNG: Erlöschen der Betriebserlaubnis

Der Betrieb des Funksystems ist nur unter Verwendung des bei Phoenix Contact erhältlichen Zubehörs zulässig. Der Einsatz von anderen Zubehörkomponenten kann zum Erlöschen der Betriebsgenehmigung führen.

Das zugelassene Zubehör für dieses Funksystem finden Sie am Produkt unter folgender Internet-Adresse: phoenixcontact.net/products.

Wir empfehlen die Multiband-Mobilfunkantenne mit Montagewinkel zur Außenmontage (TC ANT MOBILE WALL 5M, Artikel-Nr. 2702273). Beachten Sie auch die Dokumentation der Antenne unter phoenixcontact.net/product/2702273.

Beim **TC MGUARD RS2000 4G** steht das WAN nur über den Mobilfunk zur Verfügung, da keine WAN-Schnittstelle vorhanden ist. Die Mobilfunk-Funktion ist voreingestellt.
TC MGUARD RS2000 4G kann nur im Router-Modus betrieben werden.

Antennen anschließen

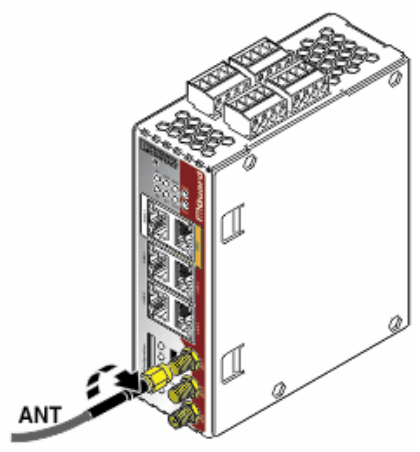


Bild 5-5 Antennenanschluss

- Schließen Sie zwei bzw. drei geeignete Antennen an die Antennenanschlüsse an:
  - Oben und Mitte: SMA für Mobilfunk (ANT1/ANT2, primäre/sekundäre Antenne)
  - Unten: RSMA (GPS)
- Wenn der Bargraph einen guten oder sehr guten Empfang anzeigt, fixieren Sie die Antenne (siehe „Bargraph“ auf Seite 86).

5.3.5 SIM-Karte

Um eine Mobilfunk-Verbindung aufzubauen, benötigt das Gerät mindestens eine gültige **Mini-SIM-Karte** im ID-000-Format, über die es sich einem Mobilfunknetz zuordnet und authentifiziert.

Die Geräte **TC MGUARD RS4000/RS2000 4G VPN** können mit zwei SIM-Karten ausgestattet werden. Die SIM-Karte in Schacht SIM 1 ist die primäre SIM-Karte, über die in der Regel die Verbindung aufgebaut wird. Wenn diese Verbindung ausfällt, kann optional auf die zweite SIM-Karte in Schacht SIM 2 zurückgegriffen werden. Sie können einstellen, ob und unter welchen Bedingungen die Verbindung dann wieder auf die primäre SIM-Karte zurückgestellt wird.

Der Zustand der SIM-Karten wird über zwei LEDs an der Front angezeigt. Die LEDs SIM1 und SIM2 leuchten grün, wenn die SIM-Karte aktiv ist. Wenn keine PIN eingegeben wurde, blinkt die LED grün.

Die Geräte **TC MGUARD RS4000/RS2000 4G ATT** und **VZW** können nur mit einer SIM-Karte im primären SIM-Kartenschacht (SIM 1) betrieben werden.

Qualität der Mobilfunk-Verbindung

Die Signalstärke der Mobilfunk-Verbindung wird über drei LEDs an der Front des Geräts angezeigt. Die LEDs funktionieren als Bargraph (siehe „Bargraph“ auf Seite 86).

Für eine stabile Datenübertragung empfehlen wir mindestens einen guten Netzempfang. Bei nur ausreichendem Netzempfang können nur SMS-Nachrichten versendet und empfangen werden.

SIM-Karte einlegen

Vom Mobilfunkanbieter (Provider) erhalten Sie eine SIM-Karte, auf der alle Daten und Services Ihres Anschlusses gespeichert sind. Wenn Sie in den USA CDMA-Netze (z. B. von Verizon Wireless) nutzen, erhalten Sie keine SIM. Stellen Sie das Gerät über die Web-Oberfläche auf einen CDMA-Provider um.

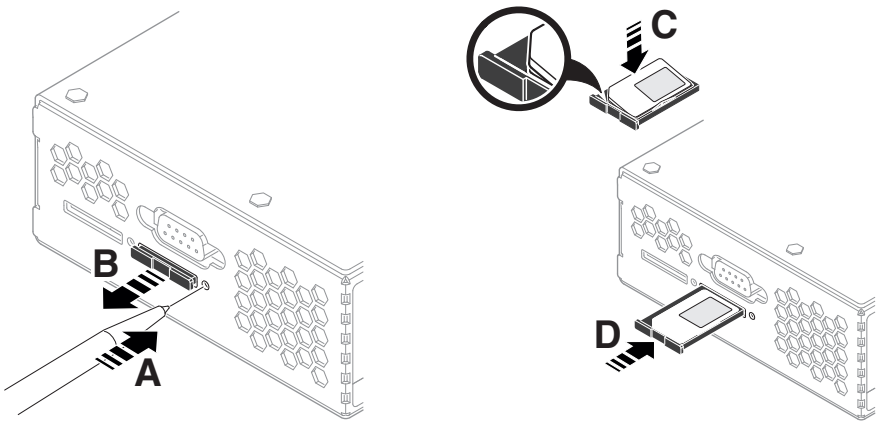


Bild 5-6 SIM-Karte einlegen

Zum Einsetzen der SIM-Karte gehen Sie wie folgt vor:

- Drücken Sie auf den Entriegelungsknopf.
- Entnehmen Sie den SIM-Karten-Halter.
- Legen Sie die SIM-Karte so ein, dass der SIM-Chip sichtbar bleibt.

- Stecken Sie den SIM-Karten-Halter mit der SIM-Karte vollständig in das Gerät, bis dieser bündig mit dem Gehäuse abschließt.

5.3.6 Versorgungsspannung anschließen

WARNUNG: Da Gerät ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach IEC 60950/EN 60950/VDE 0805 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über eine steckbare Schraubklemme, die sich oben auf dem Gerät befindet.

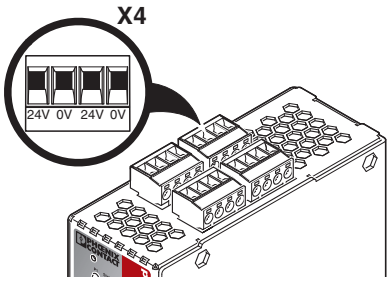
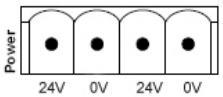
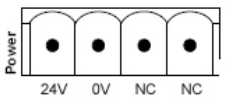


Bild 5-7 Versorgungsspannung anschließen (TC MGUARD RS4000 4G)

Tabelle 5-3 Versorgungsspannung des Geräts

TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
	

Der TC MGUARD RS4000 4G hat eine redundante Versorgungsspannung. Wenn Sie nur eine Versorgungsspannung anschließen, erhalten Sie eine Fehlermeldung.

- Nehmen Sie die steckbaren Schraubklemmen für Stromversorgung und Servicekontakte ab.
- Verdrahten Sie die Versorgungsspannungsleitungen der Schraubklemme X4 des Geräts. Ziehen Sie die Schrauben der Schraubklemmen mit 0,5 ... 0,8 Nm an.
- Stecken Sie die Steckbare Schraubklemme auf die vorgesehenen Buchsen auf der Oberseite des Geräts.

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist. Beim TC MGUARD RS4000 4G leuchtet zusätzlich die Status-Anzeige P2 bei redundantem Anschluss der Versorgungsspannung.

Das Gerät bootet die Firmware. Die LED STAT blinkt grün. Das Gerät ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die LEDs P1/P2 grün und die LED STAT blinkt grün im Heartbeat.

Redundante Spannungsversorgung (TC MGUARD RS4000 4G)

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung den TC MGUARD RS4000 4G alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der TC MGUARD RS4000 4G über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder eine geeignete Drahtbrücke zwischen den Anschlüssen anbringen.

5.4 Konfiguration vorbereiten

5.4.1 Anschlussvoraussetzungen

– Das Gerät muss an mindestens einem aktiven Netzteil angeschlossen sein.
– **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
– **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
– Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

5.5 Konfiguration im Router-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter folgender IP-Adresse erreichbar:
– https://192.168.1.1/

5.5.1 IP-Adresse 192.168.1.1

Im Router-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.
– Das Gerät ist im Auslieferungszustand.
– Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
– Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:
- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard -Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

5.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter der folgenden Adresse erreichbar:

Tabelle 5-4 Voreingestellte Adresse

Werkseinstellung	Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
TC MGUARD RS4000 4G	Router	https://192.168.1.1/
TC MGUARD RS2000 4G	Router	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die IP-Adresse des Geräts vollständig ein (siehe Tabelle 5-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die IP-Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 101).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.
  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.
  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 5-8 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

5.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

5.8 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

5.9 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

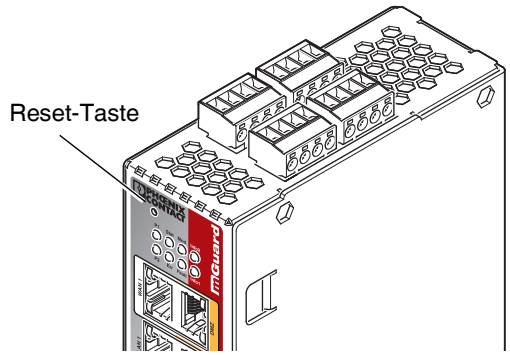


Bild 5-9 Reset-Taste

5.9.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED Err leuchtet (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

5.9.2 Recovery-Prozedur ausführen

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist. Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 5-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED STAT grün.
- Wenn die LED STAT grün erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED STAT grün
  Bei Misserfolg leuchtet die LED ERR rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

5.9.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

– **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

– alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
– diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

– Sie haben die mGuard-Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
– Diese SD-Karte ist im mGuard eingesetzt.
– Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:
  – Firmware/install-ubi.mpc83xx.p7s
  – Firmware/ubifs.img.mpc83xx.p7s
  – Firmware/ME909u-521_UPDATE_12.636.12.01.00.BIN.xz.p7s

Im Fall der Geräte **TC MGUARD RS4000/RS2000 4G ATT** und **VZW** müssen die folgende Moden-Firmware-Dateien verwendet werden:

– **TC MGUARD RS4000/RS2000 4G ATT**:
  – install-ubi.mpc83xx.p7s
  – ubifs.img.mpc83xx.p7s
  – RHL75xx.A.2.11.151600.201709111842.x7160_8_signed_DWL.dwl.xz.p7s

– **TC MGUARD RS4000/RS2000 4G VZW**:
  – install-ubi.mpc83xx.p7s
  – ubifs.img.mpc83xx.p7s
  – RHL75xx.4.03.142600.201709280115.x7160_1_signed_DWL.dwl.xz.p7s

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs Stat, Mod und Sig grün leuchten. Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware.Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED Stat blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs Stat, Mod und Sig bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED Stat leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, blinken die LEDs Stat, Mod und Sig gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie das mGuard-Gerät neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 97).

5.10 Technische Daten

Hardware-Eigenschaften	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Plattform	Freescale Netzwerkprozessor	Freescale Netzwerkprozessor
Netzwerk-Schnittstellen	4 LAN-Ports (managed) I 1 DMZ-Port I 1 WAN-Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX	4 LAN-Ports (unmanaged) Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX
Funk-Schnittstelle (TC MGUARD RS4000/RS2000 4G VPN)	WAN I GSM I GPRS I EDGE I UMTS I LTE I CDMA2000	WAN I GSM I GPRS I EDGE I UMTS I LTE I CDMA2000
Funk-Schnittstelle (TC MGUARD RS4000/RS2000 4G ATT VPN)	WAN I UMTS I LTE	WAN I UMTS I LTE
Funk-Schnittstelle (TC MGUARD RS4000/RS2000 4G VZW VPN)	WAN I LTE	WAN I LTE
SIM-Schnittstellen (1 + 2) (TC MGUARD RS4000/RS2000 4G VPN	1,8 V I 3 V, redundant	1,8 V I 3 V, redundant
SIM-Schnittstelle (1) (TC MGUARD RS4000/RS2000 4G ATT und VZW VPN)	1,8 V I 3 V	1,8 V I 3 V
Sonstige Schnittstellen	Seriell RS-232 I D-SUB 9-Stecker je 3 digitale Ein- und Ausgänge	Seriell RS-232 I D-SUB 9-Stecker je 3 digitale Ein- und Ausgänge
Speicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher
Redundanz-Optionen	optional: VPN I Router und Firewall	–
Stromversorgung	Spannungsbereich 11 ... 36 V DC, redundant	Spannungsbereich 11 ... 36 V DC
Leistungsaufnahme	typisch < 200 mA (24 V DC) maximal < 800 mA (10 V DC)	typisch < 200 mA (24 V DC) maximal < 800 mA (10 V DC)
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20	IP20
Temperaturbereich	-40 °C ... +60 °C (Betrieb) -40 °C ... +70 °C (Lagerung)	-40 °C ... +60 °C (Betrieb) -40 °C ... +70 °C (Lagerung)
Vibrationsfestigkeit nach EN 60068-2-6/IEC 60068-2-6	5g, 150 Hz, 2,5 h, in XYZ-Richtung	5g, 150 Hz, 2,5 h, in XYZ-Richtung
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	850 g	835 g

Firmware und Leistungswerte	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Firmware-Kompatibilität	TC MGUARD RS4000/RS2000 4G VPN: mGuard v8.4.1 oder höher (0x3800/0x3900) TC MGUARD RS4000/RS2000 4G VPN: mGuard v8.8.4 oder höher (0x3880/0x3980) TC MGUARD RS4000/RS2000 4G ATT und VZW: mGuard v8.7.0 oder höher Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt	
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 110 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.	
Virtual Private Network (VPN)	IPsec (IETF-Standard) optional bis zu 250 VPN-Tunnel	IPsec (IETF-Standard) bis zu 2 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 20 MBit/s Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.	

Firmware und Leistungswerte	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Datenrate (Mobilfunk)	Abhängig von der Mobilfunkverbindung ≤ 50 Mbit/s (LTE) im Upload ≤ 150 Mbit/s (LTE) im Download	
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software	
Diagnose	13 LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info, Signalstatus, SIM-Status) I Service I/OI Log-File I Remote-Syslog	

Störaussendung nach EN 61000-6-4	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Funkstörspannung nach EN 55011	EN 55011 Klasse A Einsatzgebiet Industrie	
Funkstörstrahlung nach EN 55011	EN 55011 Klasse A Einsatzgebiet Industrie	
Störaussendung	EN 61000-6-4	
Kriterium A	Normales Betriebsverhalten innerhalb der festgelegten Grenzen	
Kriterium B	Vorübergehende Beeinträchtigung des Betriebsverhaltens, die das Gerät selbst wieder korrigiert	

Sonstiges	TC MGUARD RS4000 4G	TC MGUARD RS2000 4G
Konformität	CE I Galvanische Trennung (VCC // PE)	
Besonderheiten	GPS/GLONASS-Empfänger I Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Secure Cloud ready	

6 FL MGUARD RS2000 TX/TX-B

Tabelle 6-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD RS2000 TX/TX-B	2702139

Produktbeschreibung

Der **FL MGUARD RS2000 TX/TX-B** ist ein industrieller Router mit den Funktionen statisches Routing, NAT-Routing, 1:1-NAT- Routing und Port-Forwarding.

Das Gerät unterstützt einen auswechselbaren Konfigurationsspeicher in Form einer SD-Karte (eine SD-Karte ist nicht im Lieferumfang enthalten). Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

Bild 6-1 FL MGUARD RS2000 TX/TX-B

6.1 Bedienelemente und Anzeigen

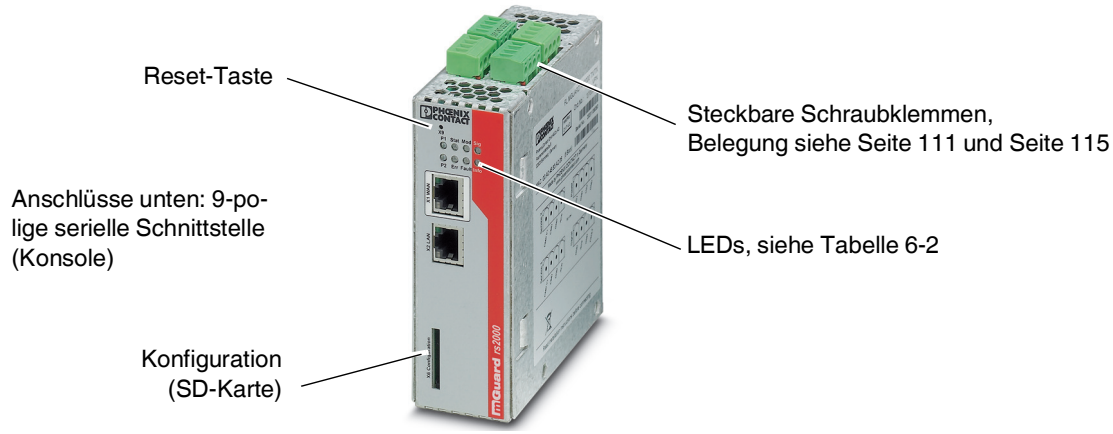


Bild 6-2 Bedienelemente und Anzeigen des Geräts

Tabelle 6-2 Anzeigen des Geräts

LED	Zustand		Bedeutung
P1	Grün	Ein	Stromversorgung 1 ist aktiv
P2	Grün	Aus	Redundante Versorgung nicht vorgesehen
STAT	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
ERR	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Reset-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe Seite 120) oder wenden Sie sich an Ihren Händler.
STAT+ ERR	Abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
SIG	–		(nicht belegt)
FAULT	Rot	Ein	Der Meldeausgang nimmt aufgrund eines Fehlers Low-Pegel ein (invertierte Logik) (siehe Seite 113). Während eines Neustarts ist der Meldeausgang inaktiv.
MOD	Grün	Aus	(Eine Verbindung per Modem ist nicht vorgesehen)
INFO	Grün	Aus	(Eine VPN-Verbindung ist nicht vorgesehen)
LAN	Grün	Ein	Die LAN/WAN LEDs befinden sich in den LAN/WAN-Buchsen (10/100 und Duplex-Anzeige) **Ethernet-Status**: Zeigt den Status des LAN- bzw. WAN-Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
WAN	Grün	Ein	

6.2 Inbetriebnahme

6.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss der mGuard richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

– Umgebungstemperatur:
  -20°C ... +60°C
– Maximale Luftfeuchtigkeit, nicht kondensierend:
  5 % ... 95 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

6.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

– Das Gerät
– Packungsbeilage
– Steckbare Schraubklemmen für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

6.3 FL MGUARD RS2000 TX/TX-B installieren

6.3.1 Montage/Demontage

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

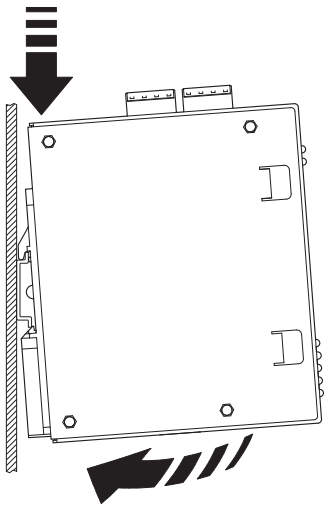


Bild 6-3 Montage des Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein. Drücken Sie das Gerät dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

6.3.2 Netzwerkverbindung anschließen

ACHTUNG: Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

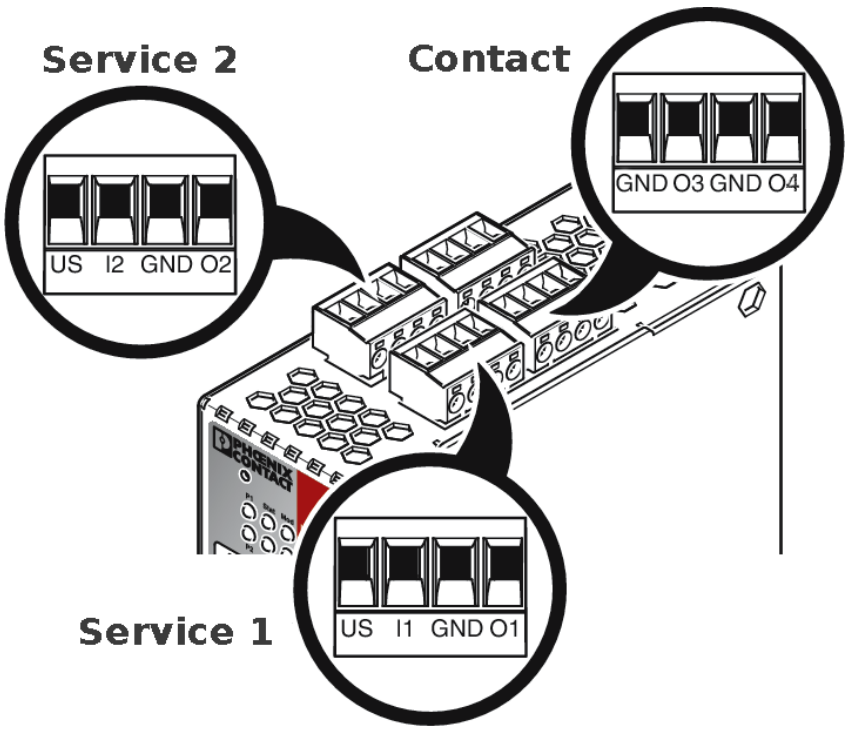
- Verbinden Sie das Gerät mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN 1 des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

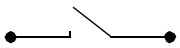
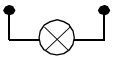
6.3.3 Servicekontakte

ACHTUNG: Schließen Sie die Spannungs- und Masseausgänge **US** (bzw. **CMD V+**) und **GND nicht** an eine externe Spannungsquelle an.

Beachten Sie, dass mit der Firmware-Version bis einschließlich 7.6.x nur die Kontakte „Service 1“ belegt sind. Die Kontakte „Service 2“ sind ab der Firmware-Version 8.1 verfügbar.

Die steckbaren Schraubklemmen der Servicekontakte können während des Betriebs des Geräts entfernt oder aufgesetzt werden.



	US	I1/I2	GND	O1/O2
Service 1 + 2	Spannungs-ausgang (+) Versorgungs-spannung	Schalt-ein-gang 11...36 V DC	Masseaus-gang (-) Versorgungs-spannung	Kurz-schlussfes-ter Schal-tausgang *
	Beispiel 		Beispiel 	

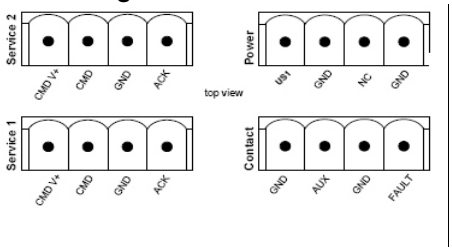
	24V	0V	NC	NC
Power	+24 V	0 V		
	siehe Kapitel 6.3.4			

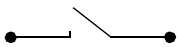
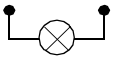
	GND	O3	GND	O4
Contact	nicht ver-wendet	nicht ver-wendet	Meldeaus-gang (-)	Meldeaus-gang (+)†

* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Die nachfolgend beschriebene Bezeichnung der Kontakte ist ebenfalls möglich:



	CMD V+	CMD	GND	ACK
Service 1 + 2	Spannungs-ausgang (+) Versorgungs-spannung	Schalt-ein-gang 11...36 V DC	Masseaus-gang (-) Versorgungs-spannung	Kurz-schlussfes-ter Schal-tausgang *
	Beispiel 		Beispiel 	

	US1	GND	NC	GND
Power	+24 V	0 V		
	siehe Kapitel 6.3.4			

	GND	AUX	GND	FAULT
Contact	nicht ver-wendet	nicht ver-wendet	Meldeaus-gang (-)	Meldeaus-gang (+)†

* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Zwischen die **Servicekontakte US** und **I** (bzw. CMD V+ und CMD) kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Die Kontakte **O1/O2 (+)** und **O4 (+)** (bzw. ACK und FAULT) sind potenzialbehaftet, dauerkurzschlussfest und liefern jeweils maximal 250 mA.

Die Schalteingänge und Schaltausgänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen von SPS-Steuerungen. Achten Sie in diesem Fall auf ein gleiches Potenzial und die Spannungs- und Stromangaben.

Die Servicekontakte können je nach verwendeter Firmware-Version für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

Servicekontakte ab Firmware-Version 8.1

Eingang/CMD I1, CMD I2

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob an die Eingänge ein Taster oder ein Ein-/Aus-Schalter angeschlossen wurde. Es können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze über den entsprechenden Schalter geschaltet werden. Auch eine Mischung von VPN-Verbindungen und Firewall-Regelsätzen ist möglich. Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und welche Firewall-Regelsätze an diesen Eingang gebunden sind.

Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von zuvor definierten VPN-Verbindungen oder der definierten Firewall-Regelsätze.

Bedienung eines angeschlossenenTasters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf EIN stellen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf AUS stellen.

Meldekontakt (Meldeausgang) O1, O2 bzw. ACK

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht und über die LED Info 1 (Ausgang/O1 bzw. ACK) oder LED Info 2 (Ausgang/O2 bzw. ACK) angezeigt werden.

Wenn VPN-Verbindungen überwacht werden, zeigt eine leuchtende LED Info, dass diese VPN-Verbindungen bestehen.

Alarmausgang O4 bzw. FAULT

Der Alarmausgang O4 überwacht die Funktion des Geräts und ermöglicht damit eine Ferndiagnose.

Die LED Fault leuchtet rot, wenn der Meldeausgang aufgrund eines Fehlers Low-Pegel einnimmt (invertierte Logik).

Durch den Alarmausgang O4 wird folgendes gemeldet, wenn das unter „Verwaltung >> Service I/O >> Alarmausgang“ aktiviert worden ist.

– Überwachung des Link-Status der Ethernet-Anschlüsse
– Überwachung des Temperaturzustandes
– Überwachung des Verbindungsstatus des internen Modems

Servicekontakte bis Firmware-Version 8.0

Meldekontakt (Meldeausgang)

Der Meldekontakt überwacht die Funktion des Geräts und ermöglicht damit eine Ferndiagnose.

Die LED FAULT leuchtet rot, wenn der Meldeausgang aufgrund eines Fehlers Low-Pegel einnimmt.

Bei dem Meldekontakt entspricht die Spannung der angelegten Versorgungsspannung. Bei der Überwachung der Ausgangsspannung wird folgendes gemeldet:

- Der Ausfall der Versorgungsspannung.
- Eine Unterschreitung des Grenzwertes bei der Stromversorgung des Geräts (Versorgungsspannung ist kleiner als 11 V).
- Überwachung des Link-Status der Ethernet-Anschlüsse, wenn dies konfiguriert worden ist. Im Lieferzustand wird die Verbindung nicht überwacht. Sie können die Überwachung einstellen (in der Web-Oberfläche unter „Verwaltung >> Systemeinstellung >> Meldekontakt“).
- Ein Fehler beim Selbsttest.

Während eines Neustarts ist der Meldekontakt abgeschaltet, bis das Gerät vollständig den Betrieb aufgenommen hat. Das gilt auch, wenn der Meldekontakt in der Software-Konfiguration unter „Manuelle Konfiguration“ auf „Geschlossen“ gestellt ist

6.3.4 Versorgungsspannung anschließen

WARNUNG: Das Gerät ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV, max. 1,5 A vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach EN 60950-1 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über eine steckbare Schraubklemme, die sich oben auf dem Gerät befindet.

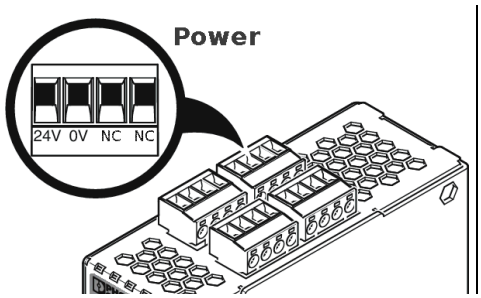


Bild 6-4 Versorgungsspannung anschließen

Anstatt der Bezeichnung **24V** wird die Bezeichnung **US1** ebenfalls verwendet.

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist.

Das Gerät bootet die Firmware. Die Status-Anzeige STAT blinkt grün. Das Gerät ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die Status-Anzeige P1 grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

6.4 Konfiguration vorbereiten

6.4.1 Anschlussvoraussetzungen

– Das Gerät muss an einem aktiven Netzteil angeschlossen sein.
– **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
– Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

6.4.2 Lokale Konfiguration bei Inbetriebnahme

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 6-3 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnitt-stelle)
FL MGUARD RS2000 TX/TX-B	Router	https://192.168.1.1/

6.4.3 IP-Adresse 192.168.1.1

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

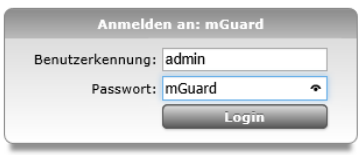


Bild 6-5 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

6.5 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

6.6 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

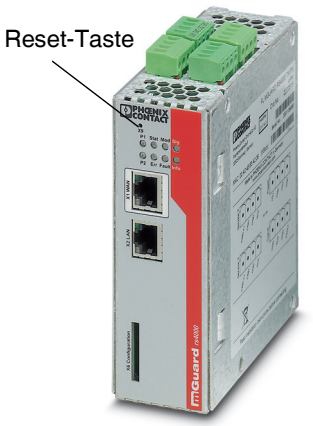


Bild 6-6 Reset-Taste

6.6.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED ERR leuchtet (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

6.6.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 6-4 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Das Gerät wird in den Router-Modus mit fester IP-Adresse zurückgesetzt.

– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Die Geräteadresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 6-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED STAT grün.
- Wenn die LED STAT grün erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED STAT grün
  Bei Misserfolg leuchtet die LED ERR rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

6.6.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

– **Alle konfigurierten Einstellungen werden gelöscht.**Das Gerät wird in den Auslieferungszustand versetzt.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

– alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
– diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

– Sie haben die Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
– Diese SD-Karte ist im Gerät eingesetzt.
– Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:

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

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs STAT, MOD und SIG grün leuchten. Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware.Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED STAT blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs STAT, MOD und SIG bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED STAT leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

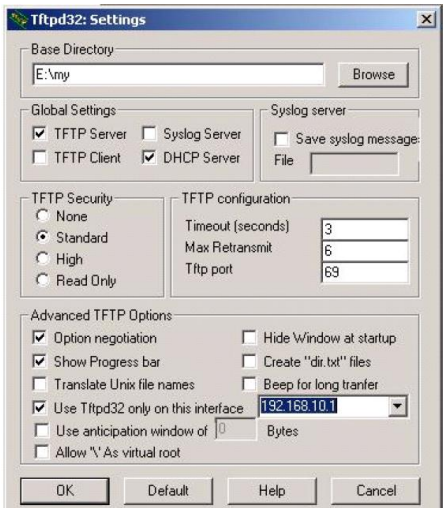
Sobald die Prozedur beendet ist, blinken die LEDs STAT, MOD und SIG gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie das mGuard-Gerät neu (siehe „Bei erfolgreichem Verbindungsaufbau“ auf Seite 117).

- Wechseln Sie auf die Registerkarte „TFTP-Server“ bzw. „DHCP-Server“ und klicken Sie dann die Schaltfläche „Settings“, um die Parameter wie folgt zu setzen:



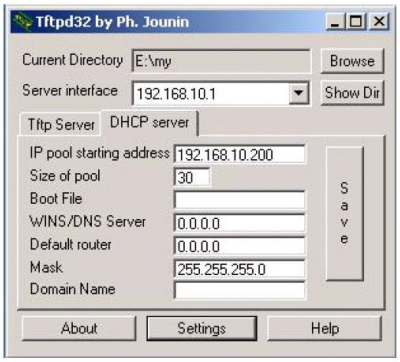


Bild 6-7 Settings

Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server.

- Installieren Sie die entsprechenden Pakete nach der Anleitung der jeweiligen Distribution.
- Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcpd.conf** folgende Einstellungen vornehmen:

  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;}

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert: **/etc/inetd.conf**

- Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

  tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/

Im Verzeichnis **/tftpboot** müssen die mGuard-Imagedateien gespeichert sein: **install.p7s, jffs2.img.p7s**

- Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** ebenfalls dort abgelegt werden.

  Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört (in der Web-Oberfläche unter „Verwaltung >> Update“).
- Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
- Wenn Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich in der entsprechenden Dokumentation.

6.7 Technische Daten

Hardware-Eigenschaften	FL MGUARD RS2000 TX/TX-B
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN Port | 1 WAN Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 | Full Duplex | Auto-MDIX
Sonstige Schnittstellen	Seriell RS-232 9-poliger D-SUB-Stecker je 2 digitale Ein- und Ausgänge (zum Teil nicht verwendet)
Speicher	128 MB RAM | 128 MB Flash SD-Karte wechselbarer Konfigurationsspeicher
Hochverfügbarkeits-Optionen	keine
Stromversorgung	Spannungsbereich 11 ... 36 V DC
Leistungsaufnahme	typisch 2,13 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20
Temperaturbereich	-20 °C ... +60 °C (Betrieb) -20 °C ... +60 °C (Lagerung)
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	725 g (TX/TX)
Gewicht (inkl. Verpackung)	900 g (TX/TX)

Firmware und Leistungswerte	FL MGUARD RS2000 TX/TX-B
Firmware-Kompatibilität	mGuard v8.x oder höher; Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz	Bi-direktionaler Durchsatz: max. 120 MBit/s
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software
Diagnose	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) Meldekontakte | Servicekontakte | Log-File | Remote-Syslog

Sonstiges	FL MGUARD RS2000 TX/TX-B
Konformität	CE | UL 508
Besonderheiten	Echtzeituhr | Temperatursensor

7 FL MGUARD RS4000 TX/TX-P

Tabelle 7-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD RS4000 TX/TX-P	2702259

Produktbeschreibung

Der **FL MGUARD RS4000 TX/TX-P** ist ein Security-Router mit intelligenter Firewall und IPsec-VPN (bis zu 250 Tunnel). Er verfügt darüber hinaus über spezielle DPI-Funktionen (Deep Packet Inspection) für OPC Classic und Modbus TCP und kann im Redundanz-Modus betrieben werden. Das Gerät ist für den Einsatz in der Prozess-Industrie mit hohen Ansprüchen an dezentrale Sicherheit und Hochverfügbarkeit konzipiert.

Der FL MGUARD RS4000 TX/TX-P unterstützt einen auswechselbaren Konfigurationsspeicher in Form einer SD-Karte. (Die SD-Karten sind nicht im Lieferumfang enthalten). Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

Bild 7-1 FL MGUARD RS4000 TX/TX-P

DPI für OPC Classic

Die Deep Packet Inspection für OPC Classic analysiert die übermittelten Pakete und nimmt gegebenenfalls Veränderungen an den Paketen vor. Über die Konfiguration kann festgelegt werden, dass über den OPC-Classic-Port 135 ausschließlich OPC-Pakete versendet werden dürfen. Die Deep Packet Inspection erkennt zuverlässig die innerhalb der ersten geöffneten Verbindung zwischen den Teilnehmern ausgehandelten TCP-Ports.

Genau diese Ports werden im Anschluss durch die Firewall geöffnet und für die OPC-Kommunikation freigegeben. Werden über diese Ports innerhalb des konfigurierbaren Timeouts keine OPC-Pakete versendet, werden die Ports wieder geschlossen. Mit fein einstellbaren Firewallregeln kann exakt definiert werden, welche Clients mit welchen Servern per OPC kommunizieren dürfen. Diese Connection-Tracking-Funktion erhöht das Security-Niveau erheblich.

DPI für Modbus TCP

Das Gerät kann Pakete ein- und ausgehende Modbus-TCP-Verbindungen prüfen und bei Bedarf filtern. Geprüft werden die Nutzdaten der eingehenden Pakete.

7.1 Bedienelemente und Anzeigen

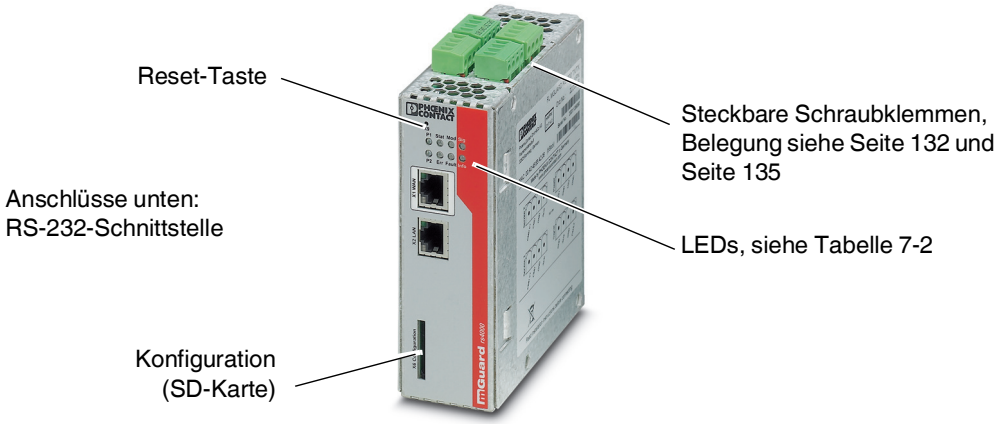


Bild 7-2 Bedienelemente und Anzeigen des Geräts

Tabelle 7-2 Anzeigen des Geräts

LED	Zustand		Bedeutung
P1	Grün	Ein	Stromversorgung 1 ist aktiv
P2	Grün	Ein	Stromversorgung 2 ist aktiv
STAT	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
ERR	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Reset-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe Seite 143) oder wenden Sie sich an Ihren Händler.
STAT+ ERR	Abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
SIG	–		(nicht belegt)
FAULT	Rot	Ein	Der Meldeausgang nimmt aufgrund eines Fehlers Low-Pegel ein (invertierte Logik) (siehe Seite 134). Während eines Neustarts ist der Meldeausgang inaktiv.
MOD	Grün	Ein	Verbindung per Modem hergestellt

Tabelle 7-2 Anzeigen des Geräts

LED	Zustand		Bedeutung
INFO	Grün	Ein	Bis Firmware-Version 8.0: Konfigurierte VPN-Verbindung ist aufgebaut Ab Firmware-Version 8.1 Konfigurierte VPN-Verbindungen sind aufgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze sind eingeschaltet
		Blinkt	Bis Firmware-Version 8.0: Konfigurierte VPN-Verbindung wird auf- oder abgebaut Ab Firmware-Version 8.1: Konfigurierte VPN-Verbindungen werden auf- oder abgebaut oder die definierten Firewall-Regelsätze werden ein- oder ausgeschaltet
LAN	Grün	Ein	Die LAN/WAN LEDs befinden sich in den LAN/WAN-Buchsen (10/100 und Duplex-Anzeige) **Ethernet-Status**. Zeigt den Status des LAN- bzw. WAN-Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
WAN	Grün	Ein	

7.2 Inbetriebnahme

7.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

- Umgebungstemperatur: –40°C ... +70°C
- 5 % ... 95 % relative Feuchte, kurzzeitige Betauung gemäß Klasse 3K7/IEC EN 60721-3-3 (außer windgetriebene Niederschläge und Eisbildung)

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

7.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

- Das Gerät
- Packungsbeilage
- Steckbare Schraubklemmen für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

7.3 FL MGUARD RS4000 TX/TX-P installieren

7.3.1 Montage/Demontage

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

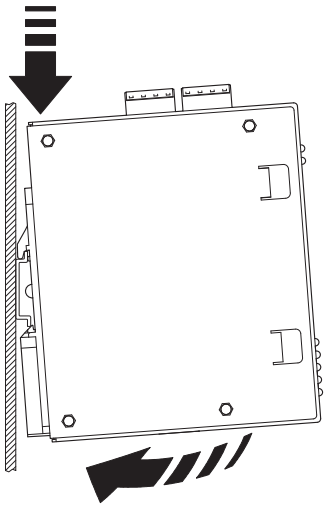


Bild 7-3 Montage des Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein. Drücken Sie das Gerät dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

7.3.2 Netzwerkverbindung anschließen

ACHTUNG: Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

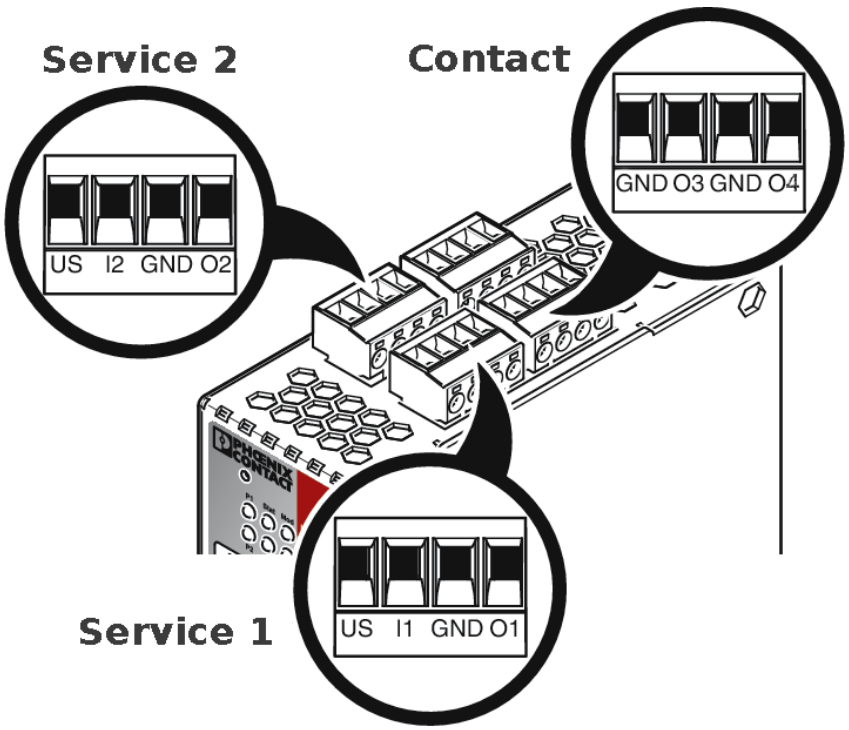
- Verbinden Sie das Gerät mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN 1 das Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

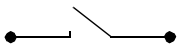
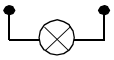
7.3.3 Servicekontakte

ACHTUNG: Schließen Sie die Spannungs- und Masseausgänge **US** (bzw. **CMD V+**) und **GND nicht** an eine externe Spannungsquelle an.

Beachten Sie, dass mit der Firmware-Version bis einschließlich 7.6.x nur die Kontakte „Service 1“ belegt sind. Die Kontakte „Service 2“ sind ab der Firmware-Version 8.1 verfügbar.

Die steckbaren Schraubklemmen der Servicekontakte können während des Betriebs des Geräts entfernt oder aufgesetzt werden.



Service 1 + 2	US	I1/I2	GND	O1/O2
	Spannungs-ausgang (+) Versorgungs-spannung	Schalt-ein-gang 11...36 V DC	Masseaus-gang (-) Versorgungs-spannung	Kurz-schlussfes-ter Schal-tausgang *
	Beispiel 		Beispiel 	

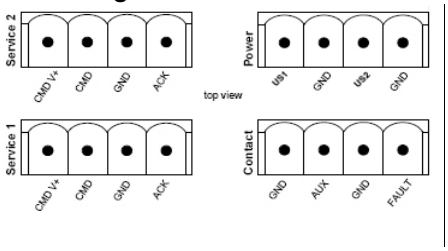
Power	24V	0V	24V	0V
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 7.3.4			

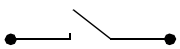
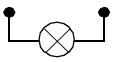
Contact	GND	O3	GND	O4
	nicht ver-wendet	nicht ver-wendet	Meldeaus-gang (-)	Meldeaus-gang (+)†

* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Die nachfolgend beschriebene Bezeichnung der Kontakte ist ebenfalls möglich:



Service 1 + 2	CMD V+	CMD	GND	ACK
	Spannungs-ausgang (+) Versorgungs-spannung	Schalt-ein-gang 11...36 V DC	Masseaus-gang (-) Versorgungs-spannung	Kurz-schlussfes-ter Schal-tausgang *
	Beispiel 		Beispiel 	

Power	US1	GND	US2	GND
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 7.3.4			

Contact	GND	AUX	GND	FAULT
	nicht ver-wendet	nicht ver-wendet	Meldeaus-gang (-)	Meldeaus-gang (+)†

* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Zwischen die **Servicekontakte US** und **I** (bzw. CMD V+ und CMD) kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Die Kontakte **O1/O2 (+)** und **O4 (+)** (bzw. ACK und FAULT) sind potenzialbehaftet, dauerkurzschlussfest und liefern jeweils maximal 250 mA

Die Schalteingänge und Schaltausgänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen von SPS-Steuerungen. Achten Sie in diesem Fall auf ein gleiches Potenzial und die Spannungs- und Stromangaben.

Die Servicekontakte können je nach verwendeter Firmware-Version für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

Servicekontakte ab Firmware-Version 8.1

Eingang/CMD I1, CMD I2

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob an die Eingänge ein Taster oder ein Ein-/Aus-Schalter angeschlossen wurde. Es können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze über den entsprechenden Schalter geschaltet werden. Auch eine Mischung von VPN-Verbindungen und Firewall-Regelsätzen ist möglich. Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und welche Firewall-Regelsätze an diesen Eingang gebunden sind.

Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von zuvor definierten VPN-Verbindungen oder der definierten Firewall-Regelsätze.

Bedienung eines angeschlossenenTasters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf EIN stellen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf AUS stellen.

Meldekontakt (Meldeausgang) O1, O2 bzw. ACK

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht und über die LED Info 1 (Ausgang/O1 bzw. ACK) oder LED Info 2 (Ausgang/O2 bzw. ACK) angezeigt werden.

Wenn VPN-Verbindungen überwacht werden, zeigt eine leuchtende LED Info, dass diese VPN-Verbindungen bestehen.

Alarmausgang O4 bzw. FAULT

Der Alarmausgang O4 überwacht die Funktion des Geräts und ermöglicht damit eine Ferndiagnose.

Die LED Fault leuchtet rot, wenn der Meldeausgang aufgrund eines Fehlers Low-Pegel einnimmt (invertierte Logik).

Durch den Alarmausgang O4 wird folgendes gemeldet, wenn das unter „Verwaltung >> Service I/O >> Alarmausgang“ aktiviert worden ist.

- Der Ausfall der redundanten Versorgungsspannung
- Überwachung des Link-Status der Ethernet-Anschlüsse
- Überwachung des Temperaturzustandes
- Überwachung des Redundanzstatus
- Überwachung des Verbindungsstatus des internen Modems

7.3.4 Versorgungsspannung anschließen

WARNUNG: Das Gerät ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach IEC 60950/EN 60950/VDE 0805 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über eine steckbare Schraubklemme, die sich oben auf dem Gerät befindet.

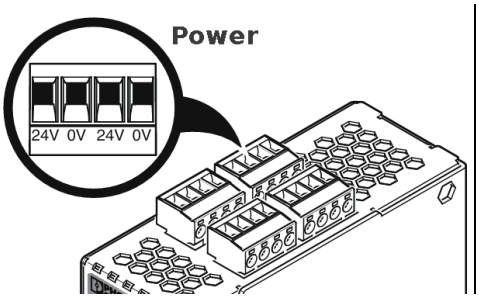


Bild 7-4 Versorgungsspannung anschließen

Anstatt der Bezeichnung **24V/24V** wird die Bezeichnung **US1/US2** ebenfalls verwendet.

Das Gerät hat eine redundante Versorgungsspannung. Wenn Sie nur eine Versorgungsspannung anschließen, erhalten Sie eine Fehlermeldung.

- Nehmen Sie die steckbaren Schraubklemmen für Stromversorgung und Servicekontakte ab.
- Schließen Sie die Servicekontakte nicht an eine externe Spannungsquelle an.
- Verdrahten Sie die Versorgungsspannungsleitungen mit der entsprechenden Schraubklemme **24V/24V** (bzw. US1/US2) des Geräts. Ziehen Sie die Schrauben der Schraubklemmen mit 0,5 ... 0,8 Nm an.
- Stecken Sie die Schraubklemmen auf die vorgesehenen Buchsen auf der Oberseite des Geräts (siehe Bild 7-4).

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist. Die Status-Anzeige P2 leuchtet zusätzlich bei redundantem Anschluss der Versorgungsspannung.

Das Gerät bootet die Firmware. Die Status-Anzeige STAT blinkt grün. Das Gerät ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die Status-Anzeigen P1/P2 grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

Redundante Spannungsversorgung

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung das Gerät alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet der das Gerät über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge **24V/24V** (bzw. US1/US2) zuführen oder eine geeignete Drahtbrücke zwischen den Anschlüssen **24V und 24V** (bzw. US1 und US2) anbringen.

7.4 Konfiguration vorbereiten

7.4.1 Anschlussvoraussetzungen

– Das Gerät muss an mindestens einem aktiven Netzteil angeschlossen sein.
– **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
– **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
– Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

7.4.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS-Verfahren (Easy Initial Setup) eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen ohne Verbindung mit einem externen Netzwerk.

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 7-3 Voreingestellte Adressen

Werkseinstellung	Netz-werk-Modus	Management-IP #1	Management-IP #2
FL MGUARD RS4000 TX/TX-P	Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät ist auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. Wenn Sie VPN-Verbindungen nutzen wollen, müssen Sie eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe Seite 139). Alternativ können Sie eine andere Stealth-Konfiguration wählen oder einen anderen Netzwerk-Modus verwenden.

7.5 Konfiguration im Stealth-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter zwei IP-Adressen erreichbar:

– https://192.168.1.1/ (siehe Seite 137)
– https://1.1.1.1/ (siehe Seite 138)

Alternativ kann per BootP eine IP-Adresse zugewiesen werden (siehe „IP-Adresse per BootP zuweisen“ auf Seite 138).

Das Gerät ist unter der Adresse https://192.168.1.1/ erreichbar, wenn die externe Netzwerkschnittstelle beim Starten nicht verbunden ist.

Das Gerät kann von Rechnern über https://1.1.1.1/ erreicht werden, wenn diese direkt oder indirekt am LAN-Port des Geräts angeschlossen sind. Dazu muss das Gerät mit LAN- und WAN-Port in ein funktionierendes Netzwerk eingebunden sein, bei dem das Standard-Gateway über den WAN-Port erreichbar ist.

– Nach einem Zugriff über die IP-Adresse 192.168.1.1 und einer erfolgreichen Anmeldung wird die IP-Adresse 192.168.1.1 als Management IP-Adresse fest eingestellt.
– Nach einem Zugriff über die IP-Adresse 1.1.1.1 oder nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

7.5.1 IP-Adresse 192.168.1.1

Im Stealth-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.

– Das Gerät ist im Auslieferungszustand.
– Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
– Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

7.5.2 IP-Adresse https://1.1.1.1/

Bei konfigurierter Netzwerkschnittstelle

Damit das Gerät über die Adresse **https://1.1.1.1/** angesprochen werden kann, muss er an eine konfigurierte Netzwerkschnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt und dabei das Standard-Gateway über den WAN-Port des Geräts erreichbar ist.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des Geräts herstellen (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 139). Fahren Sie in diesem Falle dort fort.

Nach einem Zugriff über die IP-Adresse 1.1.1.1 steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

7.5.3 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

In Kapitel 14.1 wird die IP-Adressvergabe mit Hilfe der kostenlosen Windows-Software „IP Assignment Tool“ (IPAssign.exe) erklärt.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald das Gerät eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem das Gerät eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit das Gerät erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash) ausgeführt werden.

7.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgenden Adressen erreichbar:

Tabelle 7-4 Voreingestellte Adressen

Werkseinstellung	Netz-werk-Modus	Management-IP #1	Management-IP #2
FL MGUARD RS4000 TX/TX-P	Stealth	https://1.1.1.1/	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des Geräts vollständig ein (siehe Tabelle 7-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle IP-Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 143).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.

  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.

  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.

  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.

  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbst-unterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 7-5 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

7.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an, unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

7.8 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

7.9 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

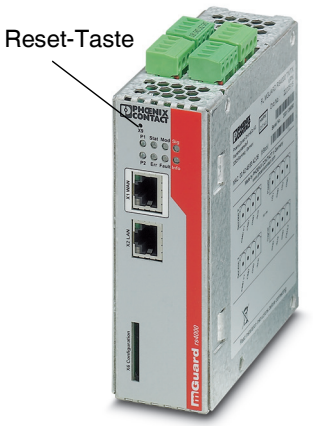


Bild 7-6 Reset-Taste

7.9.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED ERR leuchtet (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

7.9.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 7-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät wird in den Stealth-Modus mit der Werkseinstellung „mehrere Clients“ zurückgesetzt.

- Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
- Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
- Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

- Das Gerät befindet sich im Router- oder PPPoE-Modus.
- Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
- Sie kennen die aktuelle IP-Adresse des Geräts nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 7-6 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED STAT grün.
- Wenn die LED STAT grün erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED STAT grün
  Bei Misserfolg leuchtet die LED ERR rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

7.9.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ab mGuard-Firmwareversion 5.0.0 bleiben die im Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

- alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
- diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

- Sie haben die Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
- Diese SD-Karte ist im Gerät eingesetzt.
- Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:

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

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs STAT, MOD und SIG grün leuchten. Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED Stat blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs STAT, MOD und SIG bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED STAT leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, blinken die LEDs STAT, MOD und SIG gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie es neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 139).

7.10 Technische Daten

Hardware-Eigenschaften	FL MGUARD RS4000 TX/TX-P
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN-Port | 1 WAN-Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 | Full Duplex | Auto-MDIX
Sonstige Schnittstellen	Seriell RS-232 | D-SUB 9-Stecker je 2 digitale Ein- und Ausgänge
Speicher	128 MB RAM | 128 MB Flash | SD-Karte wechselbarer Konfigurationsspeicher
Redundanz-Optionen	VPN | Router und Firewall
Stromversorgung	Spannungsbereich 11 ... 36 V DC, redundant
Leistungsaufnahme	typisch 2,13 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20
Temperaturbereich	-40 °C ... +70 °C (Betrieb) -40 °C ... +70 °C (Lagerung)
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	730 g (TX/TX)
Gewicht (inkl. Verpackung)	892 g (TX/TX)

Firmware und Leistungswerte	FL MGUARD RS4000 TX/TX-P
Firmware-Kompatibilität	mGuard v8.1.0 oder höher; Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s
Virtual Private Network (VPN)	IPsec (IETF-Standard) bis zu 250 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES | 3DES | AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 20 MBit/s
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software
Diagnose	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) Meldekontakte | Servicekontakte | Log-File | Remote-Syslog

Sonstiges	FL MGUARD RS4000 TX/TX-P
Konformität	CE I FCC I UL 508 ANSI/ISA 12.12 Class I Div. 2
Zulassungen	 Class I, Zone 2, Group IIC T4 Class I, Division 2, Groups A, B, C and D T4 **The following information applies when operating this equipment in hazardous locations:** – These devices must be installed in an enclosure rated IP54 and used in an area of not more than pollution degree 2. – Use 75°C copper conductors only. – Provisions shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 40%.
Weitere Zulassungen/Approbationen	ISA-S71.04-1985 G3 Harsh Group A
Besonderheiten	Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Remote Services Portal ready

8 FL MGUARD RS4000 TX/TX VPN-M

Tabelle 8-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD RS4000 TX/TX VPN-M	2702465

Produktbeschreibung

Der **FL MGUARD RS4000 TX/TX VPN-M** ist ein Security-Router mit intelligenter Firewall und IPsec-VPN (10 Tunnel / optional bis zu 250 Tunnel). Er ist für den Einsatz in der Industrie mit hohen Ansprüchen an die dezentrale Sicherheit und die Hochverfügbarkeit konzipiert.

Der FL MGUARD RS4000 TX/TX VPN-M ist funktional identisch mit dem FL MGUARD RS4000, verfügt aber über die Zulassung für maritime Anwendungen sowie einen erweiterten Temperaturbereich.

Aktuelle Geräte-Informationen zur Zulassung für maritime Anwendungen finden Sie unter phoenixcontact.net/product/2702465.

Der FL MGUARD RS4000 TX/TX VPN-M unterstützt einen auswechselbaren Konfigurationsspeicher in Form einer SD-Karte. (Die SD-Karten sind nicht im Lieferumfang enthalten). Das lüfterlose Metallgehäuse wird auf eine Tragschiene montiert.

Folgende Konnektivitätsoptionen stehen zur Verfügung:

FL MGUARD RS4000 TX/TX VPN-M: (LAN/WAN)

Ethernet/Ethernet + VPN

Bild 8-1 FL MGUARD RS4000 TX/TX VPN-M

8.1 Bedienelemente und Anzeigen

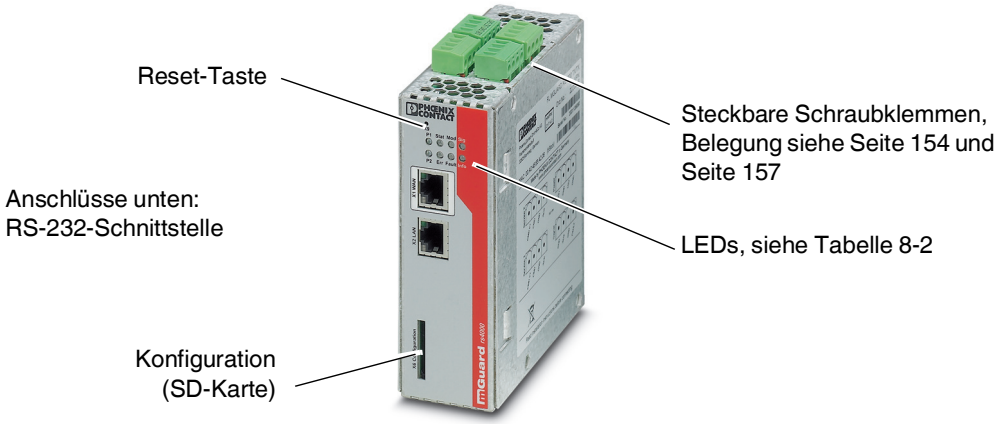


Bild 8-2 Bedienelemente und Anzeigen des Geräts

Tabelle 8-2 Anzeigen des Geräts

LED	Zustand		Bedeutung
P1	Grün	Ein	Stromversorgung 1 ist aktiv
P2	Grün	Ein	Stromversorgung 2 ist aktiv
STAT	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
ERR	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. – Dazu die Reset-Taste kurz (1,5 Sek.) drücken. – Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe Seite 166) oder wenden Sie sich an Ihren Händler.
STAT+ ERR	Abwechselnd grün-rot blinkend		**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
SIG	–		(nicht belegt)
FAULT	Rot	Ein	Der Meldeausgang nimmt aufgrund eines Fehlers Low-Pegel ein (invertierte Logik) (siehe Seite 156). Während eines Neustarts ist der Meldeausgang inaktiv.
MOD	Grün	Ein	Verbindung per Modem hergestellt

Tabelle 8-2 Anzeigen des Geräts[...]

LED	Zustand		Bedeutung
INFO	Grün	Ein	Bis Firmware-Version 8.0: Konfigurierte VPN-Verbindung ist aufgebaut Ab Firmware-Version 8.1 Konfigurierte VPN-Verbindungen sind aufgebaut oder die an Ausgang O1 definierten Firewall-Regelsätze sind eingeschaltet
		Blinkt	Bis Firmware-Version 8.0: Konfigurierte VPN-Verbindung wird auf- oder abgebaut Ab Firmware-Version 8.1: Konfigurierte VPN-Verbindungen werden auf- oder abgebaut oder die definierten Firewall-Regelsätze werden ein- oder ausgeschaltet
LAN	Grün	Ein	Die LAN/WAN LEDs befinden sich in den LAN/WAN-Buchsen (10/100 und Duplex-Anzeige) **Ethernet-Status**. Zeigt den Status des LAN- bzw. WAN-Ports. Sobald das Gerät am entsprechenden Netzwerk angeschlossen ist, zeigt kontinuierliches Leuchten an, dass eine Verbindung zum Netzwerk-Partner im LAN bzw. WAN besteht. Beim Übertragen von Datenpaketen erlischt kurzzeitig die LED.
WAN	Grün	Ein	

8.2 Inbetriebnahme

8.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

– Umgebungstemperatur:
  -40°C ... +70°C
– Maximale Luftfeuchtigkeit, nicht kondensierend:
  5 % ... 95 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

8.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

– Das Gerät
– Packungsbeilage
– Steckbare Schraubklemmen für den Stromanschluss und Ein-/Ausgänge (aufgesteckt)

8.3 FL MGUARD RS4000 TX/TX VPN-M installieren

8.3.1 Montage/Demontage

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715.

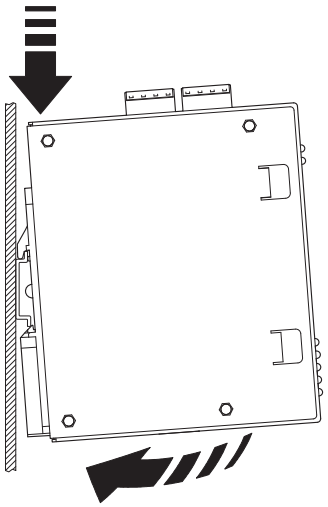


Bild 8-3 Montage des Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein. Drücken Sie das Gerät dann nach unten gegen die Tragschiene, bis er einrastet.

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

8.3.2 Netzwerkverbindung anschließen

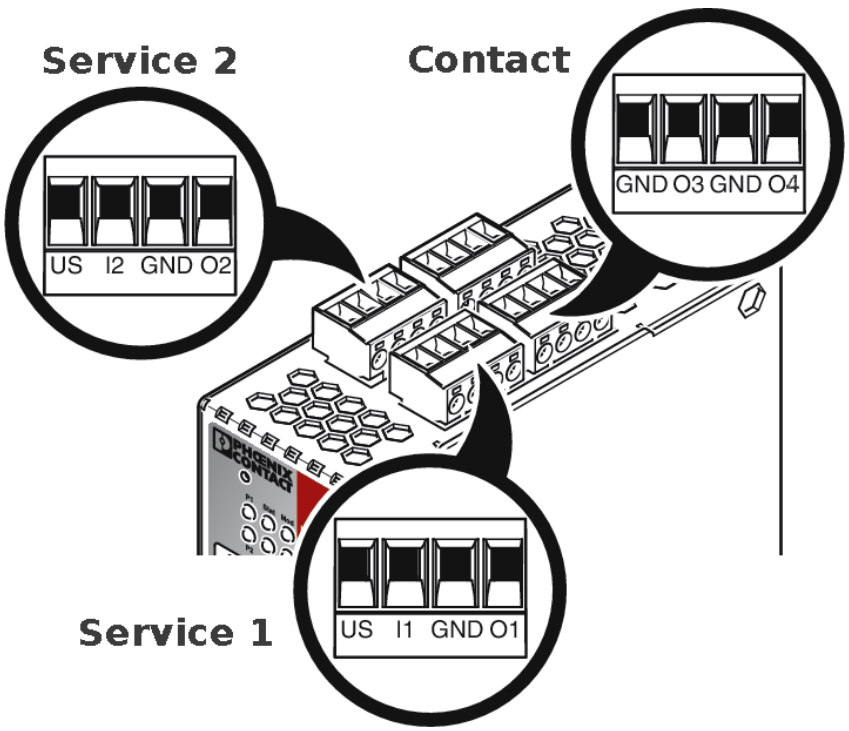
ACHTUNG: Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

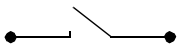
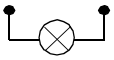
- Verbinden Sie das Gerät mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN 1 des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

8.3.3 Servicekontakte

ACHTUNG: Schließen Sie die Spannungs- und Masseausgänge **US** (bzw. **CMD V+**) und **GND nicht** an eine externe Spannungsquelle an.

Die steckbaren Schraubklemmen der Servicekontakte können während des Betriebs des Geräts entfernt oder aufgesetzt werden.



Service 1 + 2	US	I1/I2	GND	O1/O2
	Spannungs-ausgang (+) Versorgungs-spannung	Schalteingang 11...36 V DC	Masseausgang (-) Versorgungs-spannung	Kurzschlussfester Schaltausgang *
	Beispiel 		Beispiel 	

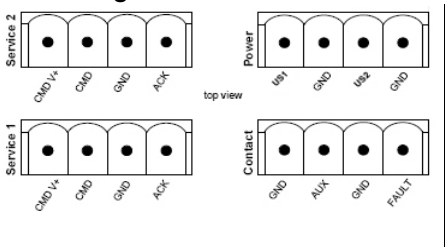
Power	24V	0V	24V	0V
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 8.3.4			

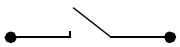
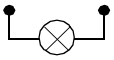
Contact	GND	O3	GND	O4
	nicht verwendet	nicht verwendet	Meldeausgang (-)	Meldeausgang (+)†

* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Die nachfolgend beschriebene Bezeichnung der Kontakte ist ebenfalls möglich:



Service 1 + 2	CMD V+	CMD	GND	ACK
	Spannungs-ausgang (+) Versorgungs-spannung	Schalteingang 11...36 V DC	Masseausgang (-) Versorgungs-spannung	Kurzschlussfester Schaltausgang *
	Beispiel 		Beispiel 	

Power	US1	GND	US2	GND
	+24 V	0 V	+24 V	0 V
	siehe Kapitel 8.3.4			

Contact	GND	AUX	GND	FAULT
	nicht verwendet	nicht verwendet	Meldeausgang (-)	Meldeausgang (+)†

* Maximal 250 mA bei 11 ... 36 V DC

† 11 V ... 36 V bei ordnungsgemäßem Betrieb, bei Fehler spannungsfrei

Zwischen die **Servicekontakte US** und **I** (bzw. CMD V+ und CMD) kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Die Kontakte **O1/O2 (+)** und **O4 (+)** (bzw. ACK und FAULT) sind potenzialbehaftet, dauerkurzschlussfest und liefern jeweils maximal 250 mA

Die Schalteingänge und Schaltausgänge können mit Signalen externer Geräte beschaltet werden, z. B. mit Signalen von SPS-Steuerungen. Achten Sie in diesem Fall auf ein gleiches Potenzial und die Spannungs- und Stromangaben.

Die Servicekontakte können je nach verwendeter Firmware-Version für verschiedene Schalt- oder Signalisierungsaufgaben verwendet werden.

Servicekontakte ab Firmware-Version 8.1

Eingang/CMD I1, CMD I2

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob an die Eingänge ein Taster oder ein Ein-/Aus-Schalter angeschlossen wurde. Es können ein oder mehrere frei wählbare VPN-Verbindungen oder Firewall-Regelsätze über den entsprechenden Schalter geschaltet werden. Auch eine Mischung von VPN-Verbindungen und Firewall-Regelsätzen ist möglich. Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und welche Firewall-Regelsätze an diesen Eingang gebunden sind.

Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von zuvor definierten VPN-Verbindungen oder der definierten Firewall-Regelsätze.

Bedienung eines angeschlossenenTasters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Einschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf EIN stellen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder Firewall-Regelsätze den Schalter auf AUS stellen.

Meldekontakt (Meldeausgang) O1, O2 bzw. ACK

Sie können über die Web-Oberfläche unter „Verwaltung >> Service I/O“ einstellen, ob bestimmte VPN-Verbindungen oder Firewall-Regelsätze überwacht und über die LED Info 1 (Ausgang/O1 bzw. ACK) oder LED Info 2 (Ausgang/O2 bzw. ACK) angezeigt werden.

Wenn VPN-Verbindungen überwacht werden, zeigt eine leuchtende LED Info, dass diese VPN-Verbindungen bestehen.

Alarmausgang O4 bzw. FAULT

Der Alarmausgang O4 überwacht die Funktion des Geräts und ermöglicht damit eine Ferndiagnose.

Die LED Fault leuchtet rot, wenn der Meldeausgang aufgrund eines Fehlers Low-Pegel einnimmt (invertierte Logik).

Durch den Alarmausgang O4 wird folgendes gemeldet, wenn das unter „Verwaltung >> Service I/O >> Alarmausgang“ aktiviert worden ist.

- Der Ausfall der redundanten Versorgungsspannung
- Überwachung des Link-Status der Ethernet-Anschlüsse
- Überwachung des Temperaturzustandes
- Überwachung des Redundanzstatus
- Überwachung des Verbindungsstatus des internen Modems

8.3.4 Versorgungsspannung anschließen

WARNUNG: Das Gerät ist für den Betrieb an einer Gleichspannung von 11 V DC ... 36 V DC/SELV vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach IEC 60950/EN 60950/VDE 0805 angeschlossen werden.

Der Anschluss der Versorgungsspannung erfolgt über eine steckbare Schraubklemme, die sich oben auf dem Gerät befindet.

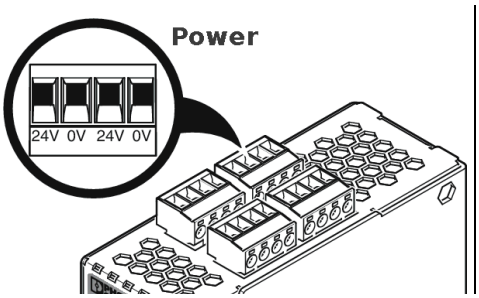


Bild 8-4 Versorgungsspannung anschließen

Anstatt der Bezeichnung **24V/24V** wird die Bezeichnung **US1/US2** ebenfalls verwendet.

Das Gerät hat eine redundante Versorgungsspannung. Wenn Sie nur eine Versorgungsspannung anschließen, erhalten Sie eine Fehlermeldung.

- Nehmen Sie die steckbaren Schraubklemmen für Stromversorgung und Servicekontakte ab.
- Schließen Sie die Servicekontakte nicht an eine externe Spannungsquelle an.
- Verdrahten Sie die Versorgungsspannungsleitungen mit der entsprechenden Schraubklemme **24V/24V** (bzw. US1/US2) des Geräts. Ziehen Sie die Schrauben der Schraubklemmen mit 0,5 ... 0,8 Nm an.
- Stecken Sie die Schraubklemmen auf die vorgesehenen Buchsen auf der Oberseite des Geräts (siehe Bild 8-4).

Die Status-Anzeige P1 leuchtet grün, wenn die Versorgungsspannung korrekt anschlossen ist. Zusätzlich leuchtet die Status-Anzeige P2 bei redundantem Anschluss der Versorgungsspannung.

Das Gerät bootet die Firmware. Die Status-Anzeige STAT blinkt grün. Das Gerät ist betriebsbereit, sobald die LEDs der Ethernet-Buchsen leuchten. Zusätzlich leuchten die Status-Anzeigen P1/P2 grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

Redundante Spannungsversorgung

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung das Gerät alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge **24V/24V** (bzw. US1/US2) zuführen oder eine geeignete Drahtbrücke zwischen den Anschlüssen **24V und 24V** (bzw. US1 und US2) anbringen.

8.4 Konfiguration vorbereiten

8.4.1 Anschlussvoraussetzungen

- Das Gerät muss an mindestens einem aktiven Netzteil angeschlossen sein.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
- **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

8.4.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS-Verfahren (Easy Initial Setup) eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen ohne Verbindung mit einem externen Netzwerk.

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 8-3 Voreingestellte Adressen

Werkseinstellung	Netz-werk-Modus	Management-IP #1	Management-IP #2
FL MGUARD RS4000 TX/TX VPN-M	Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät ist auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. Wenn Sie VPN-Verbindungen nutzen wollen, müssen Sie eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe Seite 162). Alternativ können Sie eine andere Stealth-Konfiguration wählen oder einen anderen Netzwerk-Modus verwenden.

8.5 Konfiguration im Stealth-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter zwei IP-Adressen erreichbar:

– https://192.168.1.1/ (siehe Seite 160)
– https://1.1.1.1/ (siehe Seite 160)

Alternativ kann per BootP eine IP-Adresse zugewiesen werden (siehe „IP-Adresse per BootP zuweisen“ auf Seite 161).

Das Gerät ist unter der Adresse https://192.168.1.1/ erreichbar, wenn die externe Netzwerkschnittstelle beim Starten nicht verbunden ist.

Das Gerät kann von Rechnern über https://1.1.1.1/ erreicht werden, wenn diese direkt oder indirekt am LAN-Port des Geräts angeschlossen sind. Dazu muss das Gerät mit LAN- und WAN-Port in ein funktionierendes Netzwerk eingebunden sein, bei dem das Standard-Gateway über den WAN-Port erreichbar ist.

– Nach einem Zugriff über die IP-Adresse 192.168.1.1 und einer erfolgreichen Anmeldung wird die IP-Adresse 192.168.1.1 als Management IP-Adresse fest eingestellt.
– Nach einem Zugriff über die IP-Adresse 1.1.1.1 oder nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

8.5.1 IP-Adresse 192.168.1.1

Im Stealth-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.

- Das Gerät ist im Auslieferungszustand.
- Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
- Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

8.5.2 IP-Adresse https://1.1.1.1/

Bei konfigurierter Netzwerkschnittstelle

Damit das Gerät über die Adresse **https://1.1.1.1/** angesprochen werden kann, muss er an eine konfigurierte Netzwerkschnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt und dabei das Standard-Gateway über den WAN-Port des Geräts erreichbar ist.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des Geräts herstellen (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 162). Fahren Sie in diesem Falle dort fort.

Nach einem Zugriff über die IP-Adresse 1.1.1.1 steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

8.5.3 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

In Kapitel 14.1 wird die IP-Adressvergabe mit Hilfe der kostenlosen Windows-Software „IP Assignment Tool“ (IPAssign.exe) erklärt.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald das Gerät eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem das Gerät eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit das Gerät erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash) ausgeführt werden.

8.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgenden Adressen erreichbar:

Tabelle 8-4 Voreingestellte Adressen

Werkseinstellung	Netz-werk-Modus	Management-IP #1	Management-IP #2
FL MGUARD RS4000 TX/TX VPN-M	Stealth	https://1.1.1.1/	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die IP-Adresse des Geräts vollständig ein (siehe Tabelle 8-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 166).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.

  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.

  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.

  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.

  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 8-5 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

8.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die IP-Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

8.8 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

8.9 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

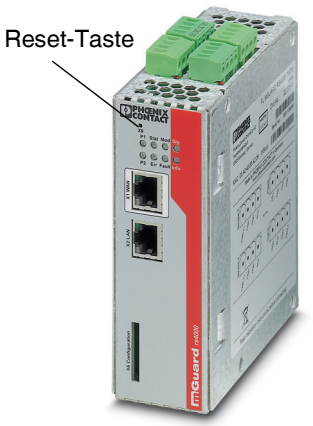


Bild 8-6 Reset-Taste

8.9.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED ERR leuchtet (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

8.9.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 8-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät wird in den Stealth-Modus mit der Werkseinstellung „mehrere Clients“ zurückgesetzt.

– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
– Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Das Gerät befindet sich im Router- oder PPPoE-Modus.
– Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
– Sie kennen die aktuelle IP-Adresse des Geräts nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 8-6 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED STAT grün.
- Wenn die LED STAT grün erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED STAT grün
  Bei Misserfolg leuchtet die LED ERR rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

8.9.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ab mGuard-Firmwareversion 5.0.0 bleiben die im Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

- alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
- diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

- Sie haben die Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
- Diese SD-Karte ist im Gerät eingesetzt.
- Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:

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

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs STAT, MOD und SIG grün leuchten. Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware. Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED Stat blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs STAT, MOD und SIG bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED STAT leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, blinken die LEDs STAT, MOD und SIG gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie es neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 162).

8.10 Technische Daten

Hardware-Eigenschaften	FL MGUARD RS4000 TX/TX VPN-M
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN-Port I 1 WAN-Port Ethernet IEEE 802.3 10/100-BaseTX RJ 45 I Full Duplex I Auto-MDIX
Sonstige Schnittstellen	Seriell RS-232 I D-SUB 9-Stecker je 2 digitale Ein- und Ausgänge
Speicher	128 MB RAM I 128 MB Flash I SD-Karte wechselbarer Konfigurationsspeicher
Redundanz-Optionen	optional: VPN I Router und Firewall
Stromversorgung	Spannungsbereich 11 ... 36 V DC, redundant
Leistungsaufnahme	typisch 2,13 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % (Betrieb, Lagerung), nicht kondensierend
Schutzart	IP20
Temperaturbereich	-40 °C ... +70 °C (Betrieb) -40 °C ... +70 °C (Lagerung)
Maße (H x B x T)	130 x 45 x 114 mm (bis Auflage Tragschiene)
Gewicht	725 g (TX/TX)
Gewicht (inkl. Verpackung)	900 g (TX/TX)

Firmware und Leistungswerte	FL MGUARD RS4000 TX/TX VPN-M	
Firmware-Kompatibilität	mGuard v8.1.8 oder höher; Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt	
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s	
Virtual Private Network (VPN)	IPsec (IETF-Standard) optional bis zu 250 VPN-Tunnel	IPsec (IETF-Standard) bis zu 2 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES I 3DES I AES-128/192/256	DES I 3DES I AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regel, bidirektionaler Durchsatz: max. 20 MBit/s	
Management Support	Web GUI (HTTPS) I Command Line Interface (SSH) I SNMP v1/2/3 I zentrale Device Management Software	
Diagnose	LEDs (Power 1 + 2, State, Error, Signal, Fault, Modem, Info) Meldekontakte I Servicekontakte I Log-File I Remote-Syslog	LEDs (Power, State, Error, Signal, Fault, Modem, Info) Meldekontakte I Servicekontakte I Log-File I Remote-Syslog

Sonstiges	FL MGUARD RS4000 TX/TX VPN-M
Konformität	CE I FCC I UL 508 ANSI/ISA 12.12 Class I Div. 2
Besonderheiten	Echtzeituhr I Trusted Platform Module (TPM) I Temperatursensor I mGuard Remote Services Portal ready

9 FL MGUARD GT/GT

Tabelle 9-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD GT/GT	2700197
FL MGUARD GT/GT VPN	2700198

Produktbeschreibung

Der **FL MGUARD GT/GT** ist hybrid nutzbar als Router/Firewall/VPN-Router sowohl über Ethernet als auch für serielle Wählverbindungen. Das Gerät ist für die Montage auf Tragschienen (nach DIN EN 60715) konzipiert und ist damit vor allem für den Einsatz im industriellem Umfeld geeignet.

VPN-Tunnel können per Software- oder Hardware-Schalter initiiert werden. Die Versorgungsspannung ist redundant anschließbar (9 V DC ... 36 V DC).

Der FL MGUARD GT/GT ist in zwei Geräteversionen lieferbar:

– als Security-Appliance FL MGUARD GT/GT
– als Security-Appliance mit VPN-Unterstützung FL MGUARD GT/GT VPN

In diesem Handbuch wird zur Vereinfachung FL MGUARD GT/GT für beide Ausführungen verwendet. Die beschriebenen Eigenschaften gelten ebenfalls für den FL MGUARD GT/GT VPN. Wenn es Abweichungen zum FL MGUARD GT/GT VPN gibt, wird darauf hingewiesen.

Bild 9-1 FL MGUARD GT/GT

9.1 Bedienelemente und Anzeigen

9.1.1 Status- und Diagnose-Anzeigen

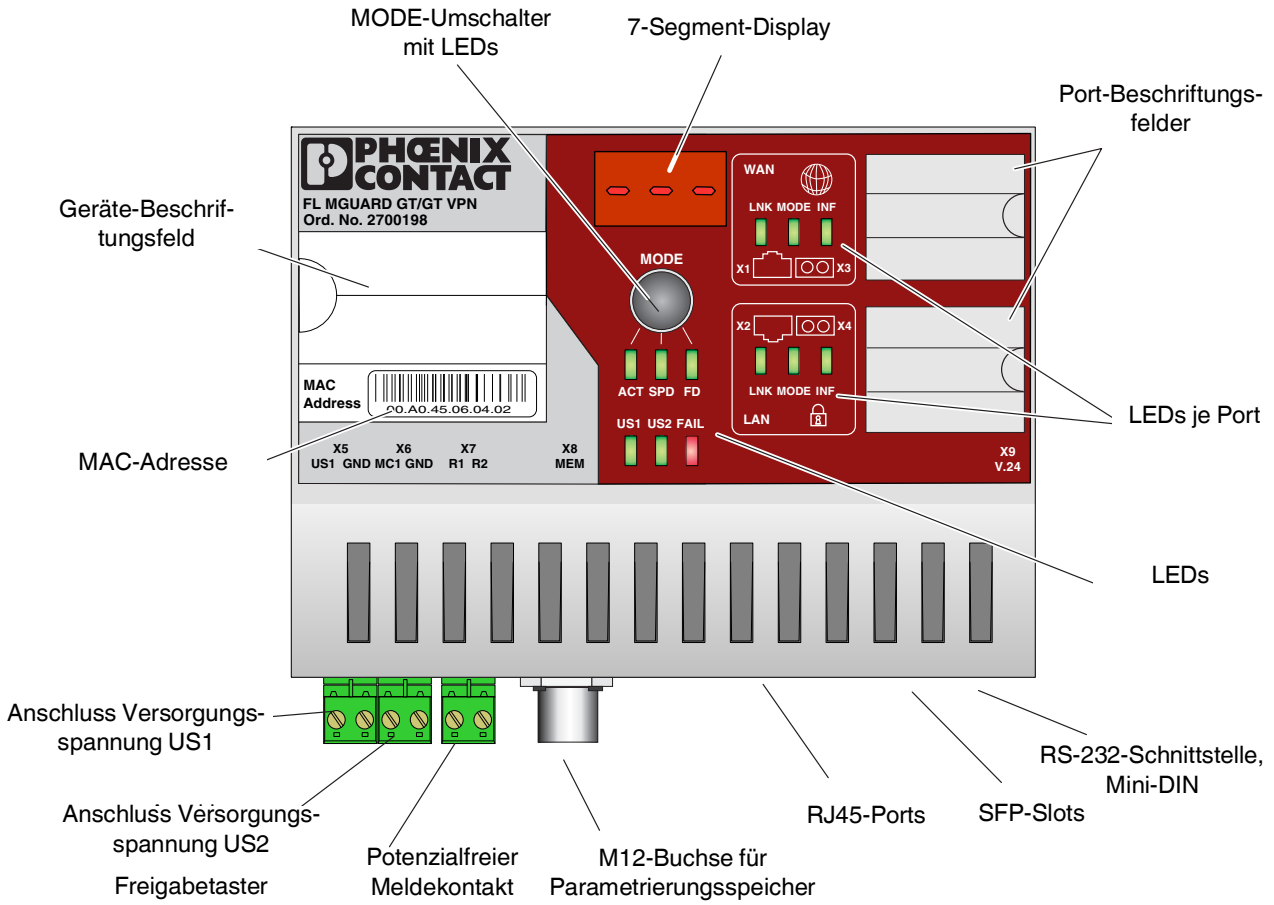


Bild 9-2 Bedienelemente und Anzeigen vom FL MGUARD GT/GT

Tabelle 9-2 Anzeigen vom FL MGUARD GT/GT

LED	Zustand		Bedeutung
US1	Grün	Ein	Versorgungsspannung 1 im Toleranzbereich
		Aus	Versorgungsspannung 1 ist zu niedrig
US2	Grün	Ein	Versorgungsspannung 2 im Toleranzbereich
		Aus	Versorgungsspannung 2 ist zu niedrig
FAIL	Rot	Ein	Meldekontakt offen, d. h. ein Fehler liegt vor
		Aus	Meldekontakt geschlossen, d. h. ein Fehler liegt nicht vor
Für den LAN- und WAN-Port befindet sich eine Link-LED auf der Front des Gerätes			
LNK (Link)	Grün	Ein	Link aktiv
		Aus	Link nicht aktiv

Tabelle 9-2 Anzeigen vom FL MGUARD GT/GT [...]

LED	Zustand		Bedeutung
Für den LAN- und WAN-Port befindet sich eine weitere LED auf der Front des Gerätes. Die Funktion der zweiten LED (MODE) je Port kann durch den MODE-Schalter umgeschaltet werden (siehe auch nachfolgendes Beispiel). Drei Umschaltmöglichkeiten stehen zur Auswahl (während des Boot-Vorgangs leuchten die Mode- und die Port-LEDs dauernd):			
ACT (Activity)	Grün	Ein	Empfang von Telegrammen
		Aus	Kein Empfang von Telegrammen
SPD (Speed)	Grün/ Orange	Ein (orange)	1000 MBit/s
		Ein (grün)	100 MBit/s (nur bei RJ45-Ports)
		Aus	10 MBit/s, wenn Link-LED aktiv (nur bei RJ45-Ports)
FD (Duplex)	Grün	Ein	Full Duplex
		Aus	Half Duplex
ACT/SPD/FD	Gelb	Blinkt	Das Gerät befindet sich im Smart-Mode (siehe „Technische Daten“ auf Seite 197)
INF (Duplex)	Grün	Ein	VPN-Tunnel etabliert
		Blinkt	VPN-Tunnel wird initialisiert
		Aus	kein VPN-Tunnel

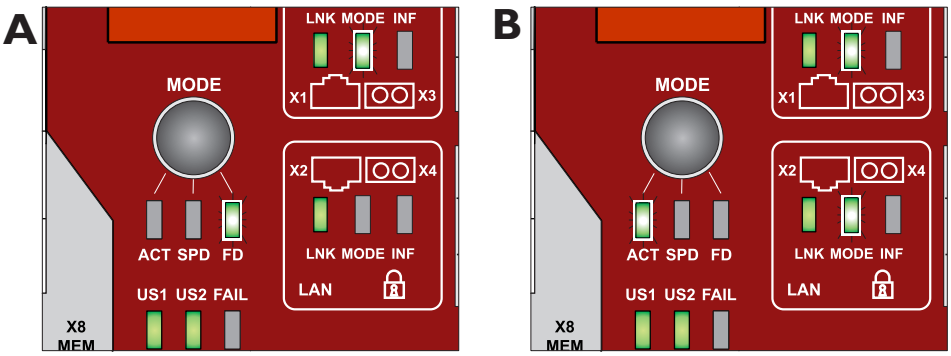


Bild 9-3 Beispiel für Status-Anzeigen beim FL MGUARD GT/GT

Beispiel:

In Bild 9-3 haben die LED-Anzeigen folgende Bedeutung:

A: Mit dem MODE-Umschalter wurde der Duplex-Mode (FD) ausgewählt; die Mode-LEDs zeigen jetzt, dass der LAN-Port im Halbduplex-Mode und der WAN-Port im Vollduplex-Mode betrieben werden.

B: Mit dem Umschalter wurde Activity (ACT) ausgewählt; die Mode-LEDs zeigen jetzt, dass auf beiden Ports eingehende Datenpakete erkannt werden.

9.1.2 Meldungen im 7-Segment-Display

Im fehlerfreien Betrieb:

Anzeige	Bedeutung
bo	Entpacken/Start der Firmware (Boot)
01	Das Gerät ist im Normalbetriebsmodus und versucht über DHCP-Requests Netzwerkparameter von einem BootP/DHCP-Server zu beziehen
03	TFTP-Download der Firmware wird durchgeführt
04	Die über das Netzwerk geladene Firmware wird ins Flash geladen
05	Die neu geladene Firmware wurde erfolgreich ins Flash gespeichert
06	Eine neue Firmware wurde erfolgreich ins Flash gespeichert, ein Rolloutscript wurde über TFTP geladen und ausgeführt
08	Das Gerät ist im Rescuemodus und versucht über DHCP-Requests Netzwerkparameter von einem BootP/DHCP-Server zu beziehen, um ein Firmwareimage anzufordern
_ _ _	Firmware wird initialisiert
- - -	Firmware läuft im Normalbetrieb
rB	Gerät führt Reboot aus
0r	Recovery-Prozedur ist gemäß des installiertem Customized-Default-Profiles deaktiviert
0d	Anwendung des Customized-Default-Profiles ist nicht möglich (z. B. weil nicht installiert)

Meldungen beim Betrieb mit Memory-Modul:

Anzeige	Bedeutung
5c	Speichere Konfigurationsdaten auf den MEM-PLUG
EC	Equal Configuration - die Konfigurationen auf dem MEM-PLUG und im Gerät sind identisch
dC	Different Configuration - die Konfigurationen auf dem MEM-PLUG und im Gerät sind unterschiedlich
0C	Der MEM-PLUG ist leer
FC	Speicherkapazität des Memory-Moduls reicht nicht aus, um die Konfiguration zu speichern
HC	Dieser MEM-PLUG ist zum Gerät inkompatibel, z. B. ein Wireless-ID-PLUG oder ein MRP-Master

Meldungen im Smart-Mode:

Smart-Mode siehe „Technische Daten“ auf Seite 197

Anzeige	Bedeutung
51	Smart-Mode „keine Änderungen“
55	Smart-Mode „Recovery-Prozedur“
56	Smart-Mode „Flash-Prozedur“
57	Smart-Mode „Customized Default Profile“

Im Fehlerfall:

Anzeige	Bedeutung	Abhilfe
41	RAM-Test-Fehler	– Führen Sie einen Spannungs-Reset durch
42	Flash-Test-Fehler	– Führen Sie einen Spannungs-Reset durch
07	Fehler beim Ausführen des Rolloutscripts	– Überprüfen Sie das Rolloutscript auf Fehler
17	Die Übertragung der Firmware per TFTP oder Xmodem ist fehlgeschlagen (Wechsel der Anzeige von „03“ auf „17“)	– Prüfen Sie die physikalische Verbindung. – Stellen Sie eine Punkt-zu-Punkt-Verbindung her. – Stellen Sie sicher, dass die Datei (mit dem angegebenen Dateinamen) existiert und sich im richtigen Verzeichnis befindet. – Prüfen Sie die IP-Adresse des TFTP-Servers. – Aktivieren Sie den TFTP-Server. – Wiederholen Sie den Download.
19	Die Übertragung der Datei wurde erfolgreich abgeschlossen, aber die Datei ist keine gültige Firmware für das Gerät	– Stellen Sie eine gültige Firmware mit dem zuvor angegebenen Dateinamen zur Verfügung – Wiederholen Sie den Download.
30	Gerätetemperatur zu hoch oder zu niedrig	– Das Gerät hat das im Web-Interface eingestellte Temperaturfenster verlassen.
49	Nicht unterstütztes oder defektes SFP-Modul	– Tauschen Sie das SFP-Modul gegen ein unterstütztes und/oder ein funktionsfähiges SFP-Modul aus
HC	Dieser MEM-PLUG ist zum Gerät inkompatibel, z. B. ein Wireless-ID-PLUG oder ein MRP-Master	– Verwenden Sie einen geeigneten MEM-PLUG

Die Punkte unter „Abhilfe“ sind Empfehlungen, die Sie nicht alle und nicht gleichzeitig durchführen müssen.

Bei allen nicht aufgeführten Meldungs-Codes kontaktieren Sie bitte Phoenix Contact.

9.2 Inbetriebnahme

9.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss der mGuard richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

- Umgebungstemperatur:
  -20 °C bis 60 °C
- Maximale Luftfeuchtigkeit, nicht kondensierend:
  95 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

9.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

- Das Gerät
- Packungsbeilage
- Klemmblock für den Stromanschluss (aufgesteckt)
- Klemmblock für den Meldekontakt, Taster

9.3 FL MGUARD GT/GT installieren

ACHTUNG: Das Gehäuse darf nicht geöffnet werden.

ACHTUNG: Die Schirmungsmasse der anschließbaren Twisted Pair-Leitungen ist elektrisch leitend mit der Frontblende verbunden.

9.3.1 Montage/Demontage

Montage

Das Gerät wird in betriebsbereitem Zustand ausgeliefert. Für die Montage und Anschluss ist folgender Ablauf zweckmäßig:

- Ziehen Sie den Klemmblock unten vom Gerät ab und verdrahten Sie die Anschlüsse, soweit nötig.
- Ziehen Sie die Schrauben der Schraubklemmen mit mindestens 0,22 Nm an. Warten Sie mit dem Einsetzen des Klemmenblocks.
- Montieren Sie das Gerät auf eine geerdete 35-mm-Tragschiene nach DIN EN 60715. Das Gerät wird durch Aufrasten auf einer geerdeten Tragschiene geerdet.

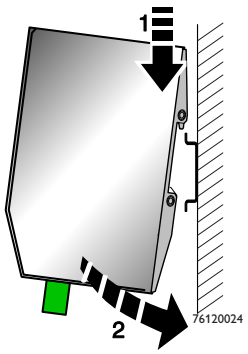


Bild 9-4 Montage des Geräts auf einer Tragschiene

- Hängen Sie dazu die obere Rastführung des Geräts in die Tragschiene ein und drücken Sie das Gerät dann nach unten gegen die Tragschiene, so dass er einrastet.
- Setzen Sie die erforderlichen verdrahteten Klemmblöcke ein.
- Nehmen Sie am LAN-Port bzw. WAN-Port die erforderlichen Netzwerkanschlüsse vor (siehe „Netzwerkverbindung anschließen“ auf Seite 178).
- Schließen Sie gegebenenfalls am Serial-Port das entsprechende Gerät an (siehe „RS-232-Schnittstelle für externes Management“ auf Seite 185).

Demontage

- Anschlüsse abnehmen bzw. trennen.
- Um das Gerät von der Tragschiene zu demontieren, stecken Sie einen Schraubendreher waagerecht unterhalb des Gehäuses in den Verriegelungsschieber, ziehen diesen – ohne den Schraubendreher zu kippen – nach unten und klappen das Gerät nach oben.

9.3.2 Netzwerkverbindung anschließen

Das Netzwerk kann über die RJ45-Ports mit Twisted-Pair-Kabel oder über SFP-Slots mit Lichtwellenleiter angeschlossen werden.

Der LAN- oder WAN-RJ45-Ports wird nach dem nächsten Reboot des Gerätes abgeschaltet, wenn ein SFP-Modul in den entsprechenden Slot eingeschoben wird.

9.3.2.1 RJ45-Ports

Der FL MGUARD GT/GT verfügt über zwei RJ45-Ports, die sowohl 10/100 MBit/s als auch 1000 MBit/s unterstützen und über die Web-Oberfläche konfigurierbar sind.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Zum Aufbau von Netzwerkverbindungen sind Kabel mit Knickschutzhülle an den Steckern empfohlen.

LAN-Port

- Verbinden Sie den lokalen Rechner oder das lokale Netzwerk mittels eines UTP-Ethernetkabels (≥ **CAT5**) mit dem LAN-Port des Geräts oder mittels SFP-Einsteckmodule (siehe „SFP-Slots“ auf Seite 180).

  Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen, dann patchen Sie den FL MGUARD GT/GT zwischen die bereits bestehende Netzwerkverbindung.

Beachten Sie, dass die Konfiguration zunächst nur über das LAN-Interface erfolgen kann und die Firewall des Geräts den gesamten IP-Datenverkehr vom WAN zum LAN-Interface unterbindet.

WAN-Port

- Benutzen Sie ein UTP-Kabel (≥ **CAT5**) oder stellen Sie die Verbindung mittels SFP-Einsteckmodule her (siehe „SFP-Slots“ auf Seite 180).
- Schließen Sie das externe Netzwerk über die WAN-Buchse an, z. B. WAN, Internet. (Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)

Es ist keine Treiber-Installation erforderlich.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

Belegung der RJ45-Ethernet-Stecker

Beachten Sie, dass für den Betrieb mit 1000 MBit/s (Gigabit) Leitungen mit vier Twisted Pairs (acht Adern), die mindestens die Anforderungen nach **CAT5e** erfüllen, zwingend erforderlich sind.

Tabelle 9-3 Pin-Belegung von RJ45-Steckern

Pin	10Base-T / 10 MBit/s	100Base-T / 100 MBit/s	1000Base-T / 1000 MBit/s
1	TD+ (Transmit)	TD+ (Transmit)	BI_DA+ (Bidirektional)
2	TD- (Transmit)	TD- (Transmit)	BI_DA- (Bidirektional)
3	RD+ (Receive)	RD+ (Receive)	BI_DB+ (Bidirektional)
4	–	–	BI_DC+ (Bidirektional)
5	–	–	BI_DC- (Bidirektional)
6	RD- (Receive)	RD- (Receive)	BI_DB- (Bidirektional)
7	–	–	BI_DD+ (Bidirektional)
8	–	–	BI_DD- (Bidirektional)

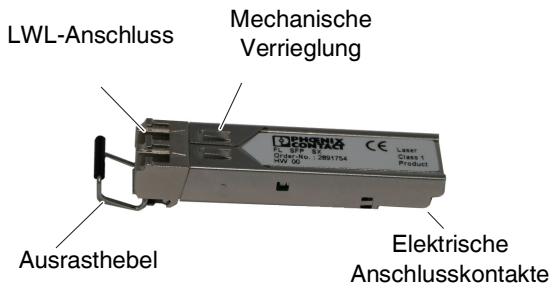
SFP-Slots

Nach dem Einschalten des Gerätes werden bestückte SFP-Module automatisch erkannt und der entsprechende RJ45-Port wird abgeschaltet. Eine Konfiguration der SFP-Module ist nicht erforderlich, da die Module automatisch konfiguriert werden (ab Firmware 8.1.x).

Das Gerät unterstützt sowohl SFP-Module mit 100 als auch mit 1000 MBit/s. Führen Sie einen Reboot aus, wenn Sie die Geschwindigkeit der verwendeten SPFs wechseln.

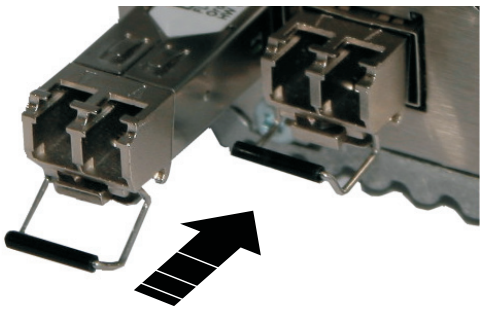
Es wird die Verwendung der folgenden SFP-Module empfohlen:

– FL SFP SX, 2891754
– FL SFP LX, 2891767
– FL SFP LH, 2989912
– FL SFP FX, 2891081
– FL SFP FX SM, 2891082



Elemente der SFP-Module

Die SFP-Slots sind zur Aufnahme von SFP-Modulen (LWL-Glasfasermodule im SFP-Format) geeignet. Über die Wahl der SFP-Module kann der Anwender festlegen, ob der Switch z. B. über Multimode- oder Singlemode-LWL-Ports verfügt.

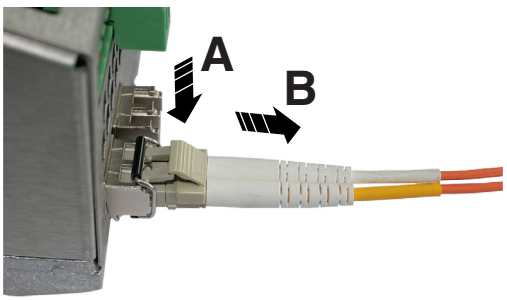


Einschieben der SFP-Module

- Schieben Sie die SFP-Module in die jeweiligen Slots.
- Achten Sie dabei auf die korrekte mechanische Ausrichtung der SFP-Module.

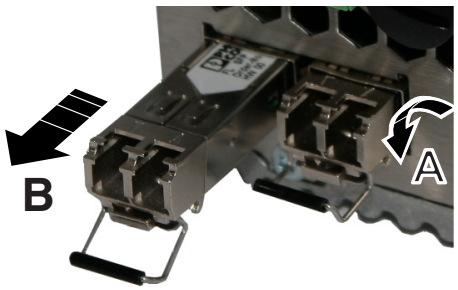
Anschließen des LWL-Kabels

- Achten Sie beim Stecken der LWL-Stecker auf die korrekte mechanische Ausrichtung.



Entfernen der LWL-Stecker

- Drücken Sie die Arretierlasche (A) und ziehen Sie den Stecker ab (B).



Entfernen der SFP-Module

- Entfernen Sie den LWL-Stecker bevor Sie das SFP-Modul entfernen.
- Klappen Sie den Ausrasthebel nach unten (A) und ziehen Sie das SFP-Modul ab (B).

9.3.3 Servicekontakte anschließen

Meldekontakt

WARNUNG: An den Meldekontakt dürfen nur SELV-Spannungskreise mit den Spannungsbeschränkungen gemäß EN 60950-1 angeschlossen werden.

Der Meldekontakt dient der Funktionsüberwachung des Geräts und ermöglicht damit eine Ferndiagnose. Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung folgendes gemeldet:

– Der Ausfall mindestens einer der zwei Versorgungsspannungen.
– Eine Grenzwertunterschreitung bei der Stromversorgung des Geräts (Versorgungsspannung 1 und/oder 2 ist kleiner als 18 V).
– Der fehlerhafte Linkstatus mindestens eines Ports. Die Meldung des Link-Status kann beim FL MGUARD GT/GT pro Port über das Management maskiert werden.
  Im Lieferzustand erfolgt keine Verbindungsüberwachung.
– Fehler beim Selbsttest.

Während eines Neustarts ist der Meldekontakt unterbrochen, bis das Gerät vollständig den Betrieb aufgenommen hat. Das gilt auch, wenn der Meldekontakt per Software-Konfiguration manuell auf „Geschlossen“ gestellt ist.

Der Switch verfügt über einen potenzialfreien Meldekontakt. Durch Öffnen des Kontaktes wird ein Fehler gemeldet.

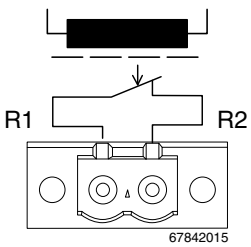


Bild 9-5 Prinzip-Schaltbild des Meldekontaktes

Freigabekontakt VPN/Firewall-Regelsatz

Versorgen Sie den Freigabetaster immer aus der Spannungsquelle, die auch den FL MGUARD GT/GT versorgt.

An den Freigabekontakt **MC1** kann ein **Taster** oder ein **Ein-/Aus-Schalter** (z. B. Schlüsselschalter) angeschlossen werden.

Der **Taster** oder **Ein-/Aus-Schalter** dient zum Auf- und Abbau von konfigurierten VPN-Verbindung oder zum Aktivieren von konfigurierten Firewall-Regelsätzen.

Bedienung eines angeschlossenen Tasters

- Zum Aufbau der VPN-Verbindung oder zum Aktivieren des Regelsatzes den Taster einige Sekunden gedrückt halten.
- Zum Abbau der VPN-Verbindung oder zum Deaktivieren des Firewall-Regelsatzes den Taster einige Sekunden gedrückt halten.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Aufbau der VPN-Verbindung/Aktivieren des Firewall-Regelsatzes den Schalter auf EIN stellen.
- Zum Abbau der VPN-Verbindung/Deaktivieren des Firewall-Regelsatzes den Schalter auf AUS stellen.

LED INF

Wenn die LED INF nicht leuchtet, wird dadurch generell signalisiert, dass die definierte VPN-Verbindung nicht besteht. Die VPN-Verbindung wurde entweder nicht aufgebaut oder ist wegen eines Fehlers ausgefallen.

Wenn die LED INF leuchtet, besteht die VPN-Verbindung.

Wenn die LED INF blinkt, wird die VPN-Verbindung gerade auf- oder abgebaut.

9.3.4 Servicekontakt ab Firmware-Version 8.1

Eingang/MC1

Sie können über die Web-Oberfläche unter "Verwaltung >> Service I/O" einstellen, ob an den Eingang ein Taster oder ein Ein-/Aus-Schalter angeschlossen wird. Eine oder mehrere frei wählbare VPN-Verbindungen bzw. ein oder mehrere Firewall-Regelsätze können über den Schalter geschaltet werden.

Über die Web-Oberfläche wird angezeigt, welche VPN-Verbindungen und welche Firewall-Regelsätze an den Eingang gebunden sind.

Der Taster oder Ein-/Aus-Schalter dient zum Auf- und Abbau von konfigurierten VPN-Verbindungen oder Firewall-Regelsätzen.

Bedienung eines angeschlossenen Tasters

- Zum Einschalten der gewählten VPN-Verbindungen oder der gewählten Firewall-Regelsätze, den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder der gewählten Firewall-Regelsätze, den Taster einige Sekunden gedrückt halten und dann den Taster loslassen.

Bedienung eines angeschlossenen Ein/Aus-Schalters

- Zum Einschalten der gewählten VPN-Verbindungen oder der gewählten Firewall-Regelsätze, den Schalter auf EIN stellen.
- Zum Ausschalten der gewählten VPN-Verbindungen oder der gewählten Firewall-Regelsätze, den Schalter auf AUS stellen.

9.3.5 Versorgungsspannung anschließen

WARNUNG: Da Gerät ist für den Betrieb an einer Gleichspannung von 18 V DC ... 32 V DC/SELV, max. 0,5 A vorgesehen.

Entsprechend dürfen an die Versorgungsanschlüsse sowie an den Meldekontakt nur SELV-Spannungskreise mit den Spannungsbeschränkungen nach IEC 60950/EN 60950/VDE 0805 angeschlossen werden.

Beachten Sie, dass mehrere Möglichkeiten beim Anschluss der Versorgungsspannung und optional des Freigabetasters/Meldekontakts (VPN/Firewall-Regelsatz) zur Auswahl stehen:

- **Einfacher Anschluss** der Versorgungsspannung
- **Redundanter Anschluss** der Versorgungsspannung

Beim FL MGUARD GT/GT können Sie an die Anschlussklemme **MCI einen VPN-Freigabetaster** bzw. einen Taster zum Schalten von Firewall-Regelsätzen anschließen.

Die Anschlussklemmen MC1/GND können entweder für den Anschluss einer (redundanten) Spannungsversorgung oder eines Freigabetasters verwendet werden.

Eine Überwachung der redundanten Versorgungsspannung und die Verwendung des MC1-Eingangs können nicht gleichzeitig erfolgen. Deaktivieren Sie in diesem Fall die Überwachung der redundanten Stromversorgung unter **Verwaltung >> Service I/O >> Alarmausgang**.

9.3.5.1 Einfacher Anschluss der Versorgungsspannung

Meldekontakt ohne Freigabetaster

Der Anschluss der Versorgungsspannung erfolgt über einen Klemmblock mit Schraubverriegelung, der sich unterhalb der Gerätefront am Gerät befindet.

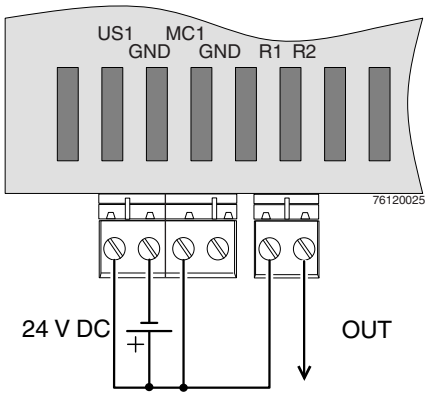


Bild 9-6 Einfacher Anschluss der Versorgungsspannung/Meldekontakt ohne Freigabetaster

9.3.5.2 Redundanter Anschluss der Versorgungsspannung

Meldekontakt ohne Freigabetaster

Die Versorgungsspannung ist redundant anschließbar. Beide Eingänge sind entkoppelt. Es besteht keine Lastverteilung. Bei redundanter Einspeisung versorgt das Netzgerät mit der höheren Ausgangsspannung das Gerät alleine. Die Versorgungsspannung ist galvanisch vom Gehäuse getrennt.

Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät über den Meldekontakt den Ausfall einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen.

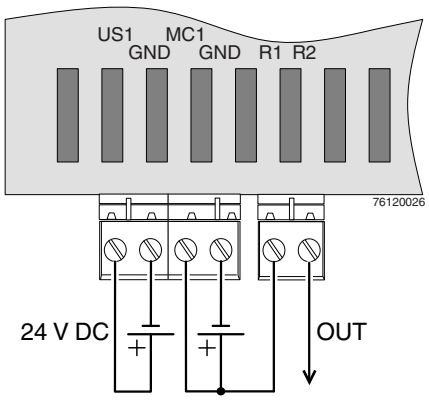


Bild 9-7 Redundanter Anschluss der Versorgungsspannung/Meldekontakt ohne Freigabetaster

9.3.5.3 Einfacher Anschluss der Versorgungsspannung mit Freigabetaster/Schalter

Versorgen Sie den Freigabetaster/Schalter immer aus der Spannungsquelle, die auch den FL MGUARD GT/GT versorgt.

Soll der Auf-/Abbau eines VPN-Tunnels oder die Aktivierung eines Firewall-Regelsatzes über einen extern am Gerät angeschlossenen Freigabetaster/Schalter initiiert werden, so ist dieser Taster/Schalter an MC1 anzuschließen.

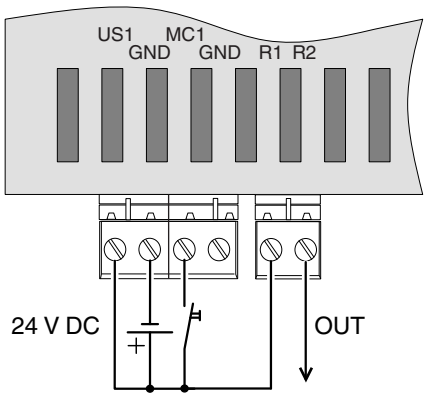


Bild 9-8 Einfacher Anschluss der Versorgungsspannung mit Freigabetaster/Schalter

9.3.5.4 Redundanter Anschluss der Versorgungsspannung mit Freigabetaster/Schalter

ACHTUNG: Verwenden Sie nur Spannungsversorgungen, die für den Parallel-Betrieb geeignet sind.

Versorgen Sie den Freigabekontakt immer aus der Spannungsquelle, die auch den **FL MGUARD GT/GT** versorgt.

Eine Überwachung der redundanten Versorgungsspannung und die Verwendung des MC1-Eingangs können nicht gleichzeitig erfolgen. Deaktivieren Sie in diesem Fall die Überwachung der redundanten Stromversorgung unter **Verwaltung >> Service I/O >> Alarmausgang**.

Soll der Auf-/Abbau eines VPN-Tunnels oder die Aktivierung eines Firewall-Regelsatzes über einen extern am Gerät angeschlossenen Freigabetaster/Schalter initiiert werden, so ist dieser Taster/Schalter an MC1 anzuschließen.

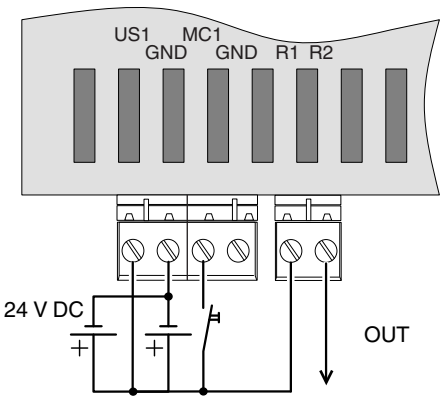


Bild 9-9 Redundanter Anschluss der Versorgungsspannung mit Freigabetaster

9.3.6 RS-232-Schnittstelle für externes Management

Über die 6-polige Mini-DIN-Buchse steht eine serielle Schnittstelle für den Anschluss einer lokalen Management-Station zur Verfügung. Damit kann über ein VT100-Terminal oder einen PC mit entsprechender Terminal-Emulation eine Verbindung zum Management-Interface hergestellt werden.

Stellen Sie folgende Übertragungsparameter ein:

Bits pro Sekunde	38400
Datenbits	8
Parität	Keine
Stoppbits	1
Flusssteuerung	Kein

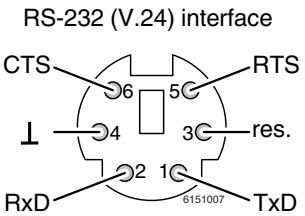


Bild 9-10 Übertragungsparameter und Belegung der RS-232-Schnittstelle

9.4 Konfiguration vorbereiten

9.4.1 Anschlussvoraussetzungen

– Das Gerät muss an mindestens einem aktivem Netzteil angeschlossen sein.
– **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
– **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
– Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

9.4.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS-Verfahren (Easy Initial Setup) eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen ohne Verbindung mit einem externen Netzwerk.

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgender Adresse erreichbar:

Tabelle 9-4 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
FL MGUARD GT/GT	Router	https://192.168.1.1/

9.4.3 Konfiguration im Router-Modus

Bei Auslieferung oder nach Zurücksetzen auf die Werkseinstellung oder Flashen des Geräts ist das Gerät über die LAN Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar.

Für einen Zugriff auf die Konfigurationsoberfläche kann es daher nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

9.5 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgender Adresse erreichbar:

Tabelle 9-5 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
FL MGUARD GT/GT	Router	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des Geräts vollständig ein (siehe Tabelle 9-5).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Flashen der Firmware / Rescue-Prozedur ausführen“ auf Seite 194).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.

  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.

  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.

  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.

  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 9-11 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

9.6 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

9.7 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 38400
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

9.8 Neustart, Recovery-Prozedur und Flashen der Firmware

Der Smart-Mode ermöglicht dem Anwender, spezielle Funktionen auszuführen, ohne Zugriff auf die Management-Interfaces zu haben.

Der FL MGUARD GT/GT bietet folgende Einstellungsmöglichkeiten über den Smart-Mode:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur ausführen

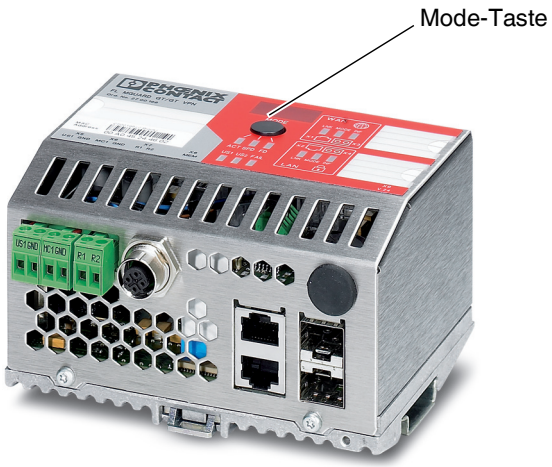


Bild 9-12 Mode-Taste

9.8.1 Funktionsauswahl mittels Mode-Taste (Smart-Mode)

Aktivieren des Smart-Modes

Über die Mode-Taste wird der Smart-Mode aufgerufen/verlassen und die gewünschte Funktion gewählt. Die drei Mode-LEDs zeigen, welche Einstellung aktuell ist und beim Verlassen des Smart-Mode berücksichtigt wird.

Aufrufen des Smart-Modes

- Trennen Sie das Gerät von der Spannungsversorgung.
- Halten Sie unmittelbar nach dem Einschalten der Versorgungsspannung die Mode-Taste **länger als zehn Sekunden** gedrückt. Die drei Mode-LEDs blinken dreimal kurz und zeigen, dass der Smart-Mode aktiviert ist.
- Zu Beginn des Smart-Modes befindet sich das Gerät zunächst im Zustand „Verlassen ohne Änderung“ („51“ im Display).

Auswahl der gewünschten Einstellung

- Um die unterschiedlichen Einstellungen zu wählen, wird die Mode-Taste kurz gedrückt und die gewünschte Betriebsart mit Hilfe eines binären Leuchtmusters der Mode-LEDs und eines Codes auf dem 7-Segment-Display ausgewählt.

Verlassen des Smart-Modes und aktivieren der Auswahl

- Zum Verlassen halten Sie die Mode-Taste mindestens fünf Sekunden gedrückt und die zuletzt gewählte Funktion wird ausgeführt.

Mögliche Funktionen im Smart-Mode

Das Gerät unterstützt die Auswahl der folgenden Funktionen im Smart-Mode (siehe auch nachfolgendes Beispiel):

Tabelle 9-6 Funktionen im Smart-Mode

Funktion	7-Segment-Display	ACT LED 1	SPD LED 2	FD LED 3
Verlassen des Smart-Mode ohne Änderung	51	Aus	Aus	**Ein**
Aktivieren der Recovery-Prozedur	55	**Ein**	Aus	**Ein**
Aktivieren der Flash-Prozedur	56	**Ein**	**Ein**	Aus
Customized-Default-Profil anwenden	57	**Ein**	**Ein**	**Ein**

9.8.2 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

Zum Starten der Funktion siehe „Funktionsauswahl mittels Mode-Taste (Smart-Mode)“. (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

9.8.3 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn die IP-Adresse, unter der das Gerät erreichbar ist, nicht bekannt ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 9-7 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Das Gerät wird in den Router-Modus mit fester IP-Adresse zurückgesetzt.

– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es im Stealth-Modus nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
– Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Das Gerät befindet sich im Router- oder PPPoE-Modus.
– Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.

– Die aktuelle IP-Adresse des Geräts ist nicht bekannt.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 9-8 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

Zum Starten der Funktion siehe „Funktionsauswahl mittels Mode-Taste (Smart-Mode)“.

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Router-Modus. Dann ist das Gerät wieder unter der entsprechenden IP-Adresse (192.168.1.1) zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

9.8.4 Flashen der Firmware / Rescue-Prozedur ausführen

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ab mGuard-Firmwareversion 5.0.0 bleiben die im Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

ACHTUNG: Zum Flashen der Firmware muss auf dem lokal angeschlossenen Rechner ein DHCP- und TFTP-Server oder ein BootP- und TFTP-Server installiert sein.

Installieren Sie den DHCP- und TFTP-Server, falls notwendig (siehe „DHCP- und TFTP-Server installieren“ auf Seite 195).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Aktion

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

Zum Starten der Funktion (Smart-Mode 56) siehe „Funktionsauswahl mittels Mode-Taste (Smart-Mode)“.

Die Statusanzeige erfolgt über das 7-Segment-Display (siehe „Meldungen im 7-Segment-Display“ auf Seite 174).

Bei Erfolg startet das Gerät nun das Rescue-System: Er sucht über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

Vom TFTP-Server wird die Datei install.mpc83xx.p7s geladen. Diese enthält die elektronisch signierte Kontrollprozedur für den Installationsvorgang. Nur signierte Dateien werden ausgeführt.

Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

Vom TFTP-Server wird die Firmware jffs2.img.mpc83xx.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

Der Vorgang dauert mehrere Minuten, in denen sich die Zahlen im 7-Segment-Display kontinuierlich ändern. Wenn im Display die **05** angezeigt wird , ist der Flash-Vorgang beendet.

Starten Sie das Gerät anschließend neu. Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie das mGuard-Gerät neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 188).

9.8.5 DHCP- und TFTP-Server installieren

Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Unter Windows

Installieren Sie das Programm, welches im Download-Bereich von phoenixcontact.net/products zu finden ist.

- Wenn der Windows-Rechner an ein Netzwerk angeschlossen ist, trennen Sie ihn von diesem.
- Kopieren Sie die Firmware in einen beliebigen leeren Ordner des Windows-Rechners.
- Starten Sie das Programm TFTPD32.EXE

Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.

- Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die mGuard-Image-Dateien gespeichert sind: **install.mpc83xx.p7s, jffs2.img.mpc83xx.p7s**
- Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** ebenfalls dort abgelegt werden.

  Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört (in der Web-Oberfläche unter „Verwaltung >> Update“).

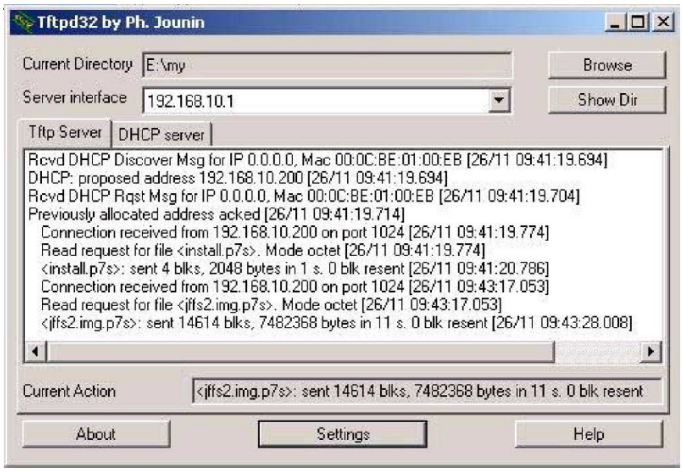
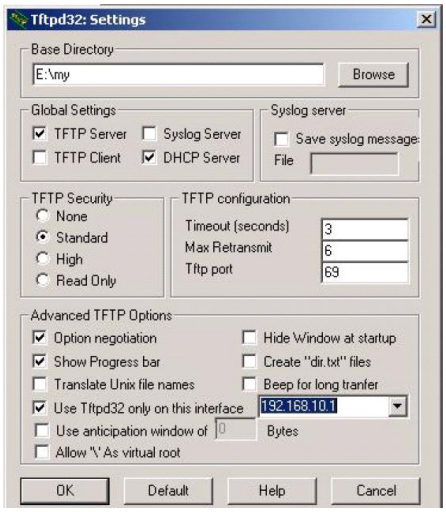


Bild 9-13 Host-IP eingeben

- Wechseln Sie auf die Registerkarte „TFTP-Server“ bzw. „DHCP-Server“ und klicken Sie dann die Schaltfläche „Settings“, um die Parameter wie folgt zu setzen:



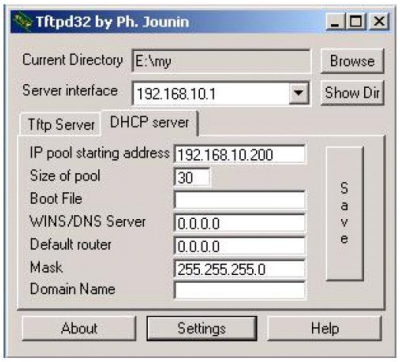


Bild 9-14 Settings

Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server.

- Installieren Sie die entsprechenden Pakete nach der Anleitung der jeweiligen Distribution.
- Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcpd.conf** folgende Einstellungen vornehmen:

  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;}

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert: **/etc/inetd.conf**

- Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

  tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/

Im Verzeichnis **/tftpboot** müssen die mGuard-Imagedateien gespeichert sein: **install.mpc83xx.p7s, jffs2.img.mpc83xx.p7s**

- Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** ebenfalls dort abgelegt werden.

  Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört (in der Web-Oberfläche unter „Verwaltung >> Update“).
- Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.
- Sollten Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich in der entsprechenden Dokumentation.

9.9 Technische Daten

Allgemeine Daten	
Funktion	Security Appliance, Firewall, Routing, 1:1-NAT; VPN (opt.), normkonform nach IEEE 802.3/802.3u/802.3ab
Firewall-Prinzip	Stateful-Inspection
SNMP	Version 2c, 3
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 350 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s
Hardwarebasierte Verschlüsselung	DES | 3DES | AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 110 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 60 MBit/s
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software | optional Schlüsselschalter (VPN)
Gehäusemaße (Breite x Höhe x Tiefe) in mm	128 x 110 x 69 (Tiefe ab Oberkante Tragschiene) 128 x 150 x 69 (Tiefe ab Oberkante Tragschiene) mit FL MEM PLUG (Zubehör)
Zulässige Betriebstemperatur	-20°C ... 60°C
Zulässige Lagertemperatur	-40°C ... +85°C
Schutzart	IP20, IEC 60529
Schutzklasse	Klasse 3 VDE 0106; IEC 60536
Luftfeuchtigkeit	
Betrieb	5 % ... 95 %, nicht kondensierend
Lagerung	5 % ... 95 %, nicht kondensierend
Luftdruck	
Betrieb	86 kPa bis 108 kPa, 1500 m ü.N.N.
Lagerung	66 kPa bis 108 kPa, 3500 m ü.N.N.
Umgebungsverträglichkeit	frei von lackbenetzungsstörenden Stoffen nach VW-Spezifikation
Einbaulage	senkrecht auf einer Norm-Tragschiene
Verbindung zur Schutzerde	durch Aufrasten auf eine geerdete Tragschiene
Gewicht	660 g typisch

Versorgungsspannung (US1 / US2 redundant)	
Anschluss	über steckbare Schraubklemme; maximaler Leiterquerschnitt = 2,5 mm^2
Nennwert	24 V DC
Zulässiger Spannungsbereich	18,0 V DC bis 32,0 V DC
Zulässige Welligkeit (innerhalb des zulässigen Spannungsbereiches)	3,6 V_{ss}
Prüfspannung	500 V DC für eine Minute
Stromaufaufnahme an US bei 24 V DC maximal	270 mA
Leistungsaufnahme maximal bei Nennspannung	6,5 W

Schnittstellen	
Anzahl der Ethernet-Ports	2, als RJ45-Port oder als SFP-Port zu betreiben
V.24-Konfigurationsschnittstelle	
Anschlussformat	Mini-DIN-Buchse

Schnittstellen [...]	
Potenzialfreier Meldekontakt	
Spannung	24 V DC
Stromtragfähigkeit	100 mA

Ethernet-Schnittstellen	
Eigenschaften der RJ45-Ports	
Anzahl	2 mit Autocrossing und Autonegotiation
Anschlussformat	8-polige RJ45-Buchse am Switch
Anschlussmedium	Twisted-Pair-Leitung mit einem Leiterquerschnitt von 0,14 mm^2 bis 0,22 mm^2
Leitungsimpedanz	100 Ohm
Übertragungsrate	10/100/1000 MBit/s
Maximale Netzsegment-Ausdehnung	100 m
Eigenschaften der SFP-Schnittstellen	
Anzahl	2
Anschlussformat	SFP Slot-Modul
Anschlussmedium	Lichtwellenleiter
Anschluss	LC-Format
Datenübertragungsrate	100 MBit/s oder 1000 MBit/s (abhängig vom verwendeten SFP-Modul)
Maximale Netzwerkausdehnung	Abhängig vom verwendeten SFP-Modul
Art der optischen Faser	Abhängig vom verwendeten SFP-Modul

Mechanische Prüfungen	
Schockprüfung nach IEC 60068-2-27	Betrieb: 30g/11 ms Halbsinus-Schockimpuls Lagerung/Transport: 50g, Halbsinus-Schockimpuls
Vibrationsfestigkeit nach IEC 60068-2-6	Betrieb/Lagerung/Transport: 5g, 57 - 150 Hz
Freier Fall nach IEC 60068-2-32	1 m

Konformität zur EMV-Richtlinie 2004/108/EG und zur Niederspannungsrichtlinie 2006/95/EG

Prüfung der Störfestigkeit nach EN 61000-6-2[1]

				Prüfschärfegrad
Entladung statischer Elektrizität (ESD)	EN 61000-4-2	Kriterium B[2]	Kontaktentladung	2
			Luftentladung	2
			Indirekte Entladung	3
Elektromagnetisches HF-Feld	EN 61000-4-3	Kriterium A[3]		3
Schnelle Transienten (Burst)	EN 61000-4-4	Kriterium B[2]	Datenleitungen	2
			Spannungsversorgung	3
Stoßstrombelastung (Surge)	EN 61000-4-5	Kriterium B[2]	Datenleitungen	2
			Spannungsversorgung	1
Leitungsgeführte Störgrößen	EN 61000-4-6	Kriterium A[3]	Prüfschärfegrad 3	

Prüfung der Störabstrahlung nach EN 61000-6-4

Störaussendung Gehäuse	EN 55011[4]	Klasse A[5]		
Störaussendung	EN 55022	Klasse B[6]		

[1] EN 61000 entspricht der IEC 61000

[2] Kriterium B: Vorübergehende Beeinträchtigung des Betriebsverhaltens, die das Gerät selbst korrigiert.

[3] Kriterium A: Normales Betriebsverhalten innerhalb der festgelegten Grenzen.

[4] EN 55011 entspricht der CISPR11

[5] Klasse A: Einsatzgebiet Industrie, ohne besondere Installationsmaßnahmen

[6] Klasse B: Wohnbereich

Weitere Zertifizierungen

RoHS	EEE 2002/95/EC. - WEEE 2002/96/EC

10 FL MGUARD PCI(E)4000

Tabelle 10-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD PCI4000	2701274
FL MGUARD PCI4000 VPN	2701275
FL MGUARD PCIE4000	2701277
FL MGUARD PCI4000 VPN	2701278

Produktbeschreibung

Der **FL MGUARD PCI(E)4000** hat die Form einer PCI-kompatiblen Steckkarte. Es gibt ihn in zwei Ausführungen:

– **FL MGUARD PCI4000 (VPN)** für Geräte oder Maschinen mit PCI-Bus
– **FL MGUARD PCI4000 VPN** für Geräte oder Maschinen mit PCI-Express-Bus

In diesem Handbuch wird zur Vereinfachung **FL MGUARD PCI4000** für beide Ausführungen verwendet.

Der **FL MGUARD PCI4000** eignet sich für die dezentrale Absicherung von Industrie- und Panel-PCs, einzelnen Maschinen oder Industrie-Robotern. Er verfügt über einen Konfigurationsspeicher in Form einer wechselbaren SD-Karte, die an der Frontseite gut zugänglich ist.

Bild 10-1 FL MGUARD PCI4000

10.1 Bedienelemente und Anzeigen

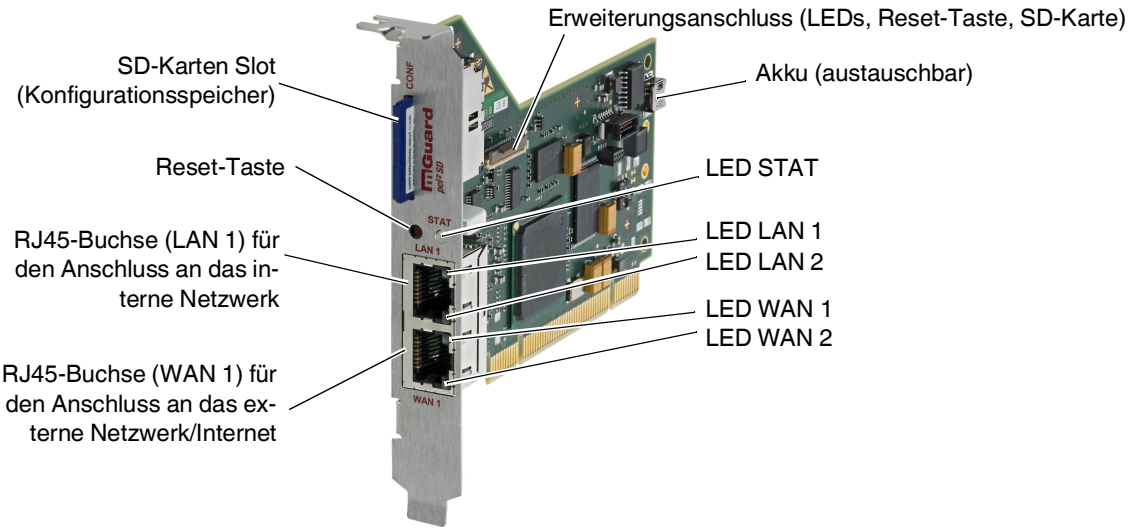


Bild 10-2 Bedienelemente und Anzeigen vom FL MGUARD PCI4000

Tabelle 10-2 Anzeigen vom FL MGUARD PCI4000

LEDs	Zustand		Bedeutung
WAN 1 **LAN 1**	Grün	Ein	Vollduplex
		Aus	Halbduplex
WAN 2 **LAN 2**	Gelb	Ein	10 MBit/s
		Blinkt	10 MBit/s, Datenübertragung aktiv
	Grün	Ein	100 MBit/s
		Blinkt	100 MBit/s, Datenübertragung aktiv
LAN 1 **LAN 2** **WAN 1**	Diverse LED-Leuchtcodes		**Recovery-Prozedur/Flashen** Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 214.
STAT	Rot/Grün	Blinkt	**Bootprozess.** Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktionsfähig.
	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. • Dazu die Reset-Taste kurz (1,5 Sek.) drücken. • Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe „Recovery-Prozedur ausführen“ auf Seite 215) oder wenden Sie sich an Ihren Händler.

10.2 Inbetriebnahme

10.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Anschlusshinweise

- Beim FL MGUARD PCI4000 muss Ihr PC einen freien PCI-Slot (3,3 V oder 5 V) bereitstellen.
- Anschlusskabel nicht knicken. Den Netzwerkstecker nur zum Verbinden mit einem Netzwerk benutzen.

ACHTUNG: Umgebungsbedingungen passend auswählen

- Umgebungstemperatur:
  0 °C ... +60 °C (FL MGUARD PCI4000 mit Akku)
  0 °C ... +70 °C (FL MGUARD PCI4000 ohne Akku)
- Maximale Luftfeuchtigkeit, nicht kondensierend:
  5 % ... 95 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

10.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

- FL MGUARD PCI4000
- Packungsbeilage

10.3 FL MGUARD PCI4000 installieren

WARNUNG: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen durchzuführen.

WARNUNG: Die sichere Trennung von berührungsgefährlichen Stromkreisen ist nur gewährleistet, wenn die angeschlossenen Geräte die Anforderungen der VDE 0106-101 (Sichere Trennung) erfüllen. Für die sichere Trennung sind die Zuleitungen getrennt von berührungsgefährlichen Stromkreisen zu führen oder zusätzlich zu isolieren.

10.3.1 Hardware einbauen

ACHTUNG: Elektrostatische Entladung

Berühren Sie vor dem Einbau den freien Metallrahmen des PCs, in den Sie den FL MGUARD PCI4000 einbauen wollen, um Ihren Körper elektrostatisch zu entladen.

Das Gerät enthält Bauelemente, die durch elektrostatische Entladung beschädigt oder zerstört werden können. Beachten Sie beim Umgang mit dem Gerät die notwendigen Sicherheitsmaßnahmen gegen elektrostatische Entladung (ESD) nach EN 61340-5-1 und IEC 61340-5-1.

FL MGUARD PCI4000: Aufbau

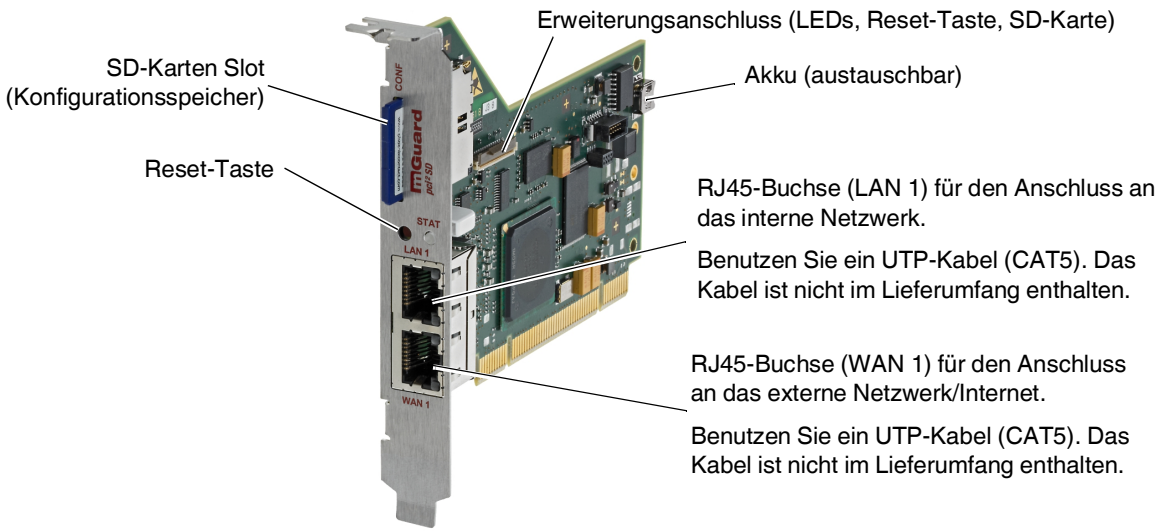


Bild 10-3 Aufbau FL MGUARD PCI4000

- Bauen Sie den FL MGUARD PCI4000 in einen freien PCI- oder PCI-Express-Steckplatz ein. Beachten Sie dabei die Hinweise in der Dokumentation zu Ihrem System.

10.4 Konfiguration vorbereiten

10.4.1 Anschlussvoraussetzungen

- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss folgende Voraussetzungen erfüllen:
  - Der Rechner muss am LAN-Anschluss des Geräts angeschlossen sein oder über das lokale Netzwerk mit dem Gerät verbunden sein.
- **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

10.4.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS-Verfahren (Easy Initial Setup) eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen ohne Verbindung mit einem externen Netzwerk.

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 10-3 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät ist auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. Wenn Sie VPN-Verbindungen nutzen wollen, müssen Sie eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe Seite 211). Alternativ können Sie eine andere Stealth-Konfiguration wählen oder einen anderen Netzwerk-Modus verwenden.

10.5 Konfiguration im Stealth-Modus

Der FL MGUARD PCI4000 kann auf drei unterschiedliche Arten in Betrieb genommen werden:

– Gerät im Stealth-Modus in Betrieb nehmen (Standard)
– Gerät über temporäre Management IP-Adresse in Betrieb nehmen
– Gerät per BootP in Betrieb nehmen

10.5.1 Gerät im Stealth-Modus in Betrieb nehmen (Standard)

Schalten Sie das Gerät zwischen eine bestehende Netzwerkverbindung.

Sie benötigen dafür geeignete UTP-Kabel (CAT5) für den Anschluss an die LAN- und WAN-Schnittstelle. Die Kabel sind nicht im Lieferumfang enthalten.

- Verbinden Sie die interne Netzwerkschnittstelle (LAN 1) des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerkanschluss des internen Netzwerks.
- Verbinden Sie die externe Netzwerkschnittstelle (WAN 1) des Geräts mit dem externen Netzwerk, z. B. dem Internet.

Die Status-Anzeige STAT leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.

Das Gerät bootet die Firmware. Die Status-Anzeige STAT blinkt währenddessen grün.

Das Gerät ist betriebsbereit, sobald die unteren LEDs der Ethernet-Buchsen leuchten. Zusätzlich blinkt die Status-Anzeige STAT grün im Heartbeat.

Sie können eine fehlende Verbindung zum internen oder externen Netzwerk dadurch erkennen, dass die unteren LEDs in den Ethernet-Buchsen nicht leuchten. Wenn keine LED leuchtet, fehlt die Versorgungsspannung.

Das Gerät wird per Web-Browser konfiguriert, der auf dem lokal angeschlossenen Rechner (z. B. dem Schützling) ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist voreingestellt unter der folgenden Adresse erreichbar: https://1.1.1.1/

FL MGUARD PCI4000 konfigurieren

- Geben Sie im Browser die folgende Adresse ein: https://1.1.1.1/

Die Verbindung zum FL MGUARD PCI4000 wird hergestellt. (Wenn nicht, siehe Kapitel 10.5.2).

Ein Sicherheitshinweis wegen eines angeblich ungültigen/nicht vertrauenswürdigen Zertifikats wird angezeigt. Diese Meldung resultiert aus der Verwendung eines mGuard-eigenen Zertifikats von Phoenix Contact, das dem Browser noch unbekannt ist, aber zur Verschlüsselung der Kommunikation benötigt wird.

- Quittieren Sie den Hinweis mit
  „Dieses Zertifikat immer/temporär akzeptieren“ (Mozilla Firefox),
  „Laden dieser Website fortsetzen“ (MS Internet Explorer),
  „Trotzdem Fortfahren“ (Google Chrome).
- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 10-4 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern (in der Web-Oberfläche unter „Authentifizierung >> Administrative Benutzer“).

10.5.2 FL MGUARD PCI4000 über eine temporäre Management IP-Adresse in Betrieb nehmen

Wenn im Erstinbetriebnahme-Modus der FL MGUARD PCI4000 ohne ein funktionierendes externes Netzwerk angeschlossen wird, so ist das Gerät unter der Adresse https://1.1.1.1/ **nicht** erreichbar.

Der FL MGUARD PCI4000 ist in diesem Fall automatisch über die Management IP-Adresse 192.168.1.1/24 erreichbar. Das gilt sowohl für die interne (LAN 1) als auch externe (WAN 1) Netzwerkschnittstelle. Ein Adressenkonflikt an der externen Netzwerkschnittstelle ist nicht möglich, solange WAN 1 nicht an ein funktionierendes Netzwerk angeschlossen wird. Diese Management IP-Adresse ist normalerweise nicht persistent.

Wenn nach dem Hochfahren des FL MGUARD PCI4000 die externe Netzwerkschnittstelle (WAN 1) nachträglich verbunden wird, bleibt die Management IP-Adresse bestehen. In diesem Fall ist ein Adressenkonflikt mit bereits bestehenden Adressen im externen Netzwerk möglich.

FL MGUARD PCI4000 ohne externes Netzwerk in Betriebe nehmen

- Verbinden Sie die interne Netzwerkschnittstelle (LAN 1) des FL MGUARD PCI4000 mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks.
- Trennen Sie die externe Netzwerkschnittstelle (WAN 1) des FL MGUARD PCI4000 vom externen Netzwerk (WAN).
- Schalten Sie das System ein. Die LED STAT leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.

Das Gerät bootet die Firmware. Die LED STAT blinkt grün.

Konfigurationsrechner anpassen

Um den FL MGUARD PCI4000 für die Konfiguration erreichen zu können, müssen Sie den Konfigurationsrechner an die Management IP-Adresse des FL MGUARD PCI4000 angepassen

Beispiel für Microsoft Windows XP:

- Stellen Sie im Dialogfeld „Eigenschaften von Internetprotokoll (TCP/IP)“ der betreffenden Netzwerkschnittstelle des Konfigurationsrechners Folgendes ein:

IP-Adresse:	192.168.1.10
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.2

- Geben Sie im Browser die zugewiesene Adresse ein: https://192.168.1.1/
- Konfigurieren Sie das Gerät wie unter „FL MGUARD PCI4000 konfigurieren“ auf Seite 207 beschrieben.

10.5.3 FL MGUARD PCI4000 per BootP in Betrieb nehmen

Der FL MGUARD PCI4000 startet bei der Erstinbetriebnahme immer zusätzlich einen BootP-Clienten an der internen Netzwerkschnittstelle (LAN 1). Der BootP-Client ist kompatibel zu den BootP-Servern „IPAssign“ von Phoenix Contact sowie „DHCPD“ unter Linux.

Diese Software steht unter der Adresse phoenixcontact.net/products zum kostenlosen Download bereit.

Die IP-Adressvergabe mit Hilfe von IPAssign wird in Kapitel „Vergabe der IP-Adresse mit IPAssign.exe“ auf Seite 273 ausführlich beschrieben.

Wenn ein nicht konfigurierter FL MGUARD PCI4000 nach dem Hochfahren einen BootP-Server erreicht, dann wird dem FL MGUARD PCI4000 über das BootP-Protokoll eine IP-Adresse, eine Subnetzmaske und optional ein Standard-Gateway der internen Netzwerkschnittstelle zugewiesen. Diese Parameter werden persistent im Gerät gespeichert, welches dann ab sofort darunter erreichbar ist.

- Geben Sie im Browser die per BootP zugewiesene Adresse ein: z. B. https://192.168.1.1/

Konfigurieren Sie das Gerät wie unter „FL MGUARD PCI4000 konfigurieren“ auf Seite 207 beschrieben.

10.5.4 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

In Kapitel 14.1 wird die IP-Adressvergabe mit Hilfe der kostenlosen Windows-Software „IP Assignment Tool“ (IPAssign.exe) erklärt.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald das Gerät eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem das Gerät eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit das Gerät erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash) ausgeführt werden.

10.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgenden Adressen erreichbar:

Tabelle 10-4 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
FL MGUARD PCI4000	Stealth	https://1.1.1.1/	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des Geräts vollständig ein (siehe Tabelle 10-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 215).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.
  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.
  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 10-5 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

10.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die IP-Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

10.8 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

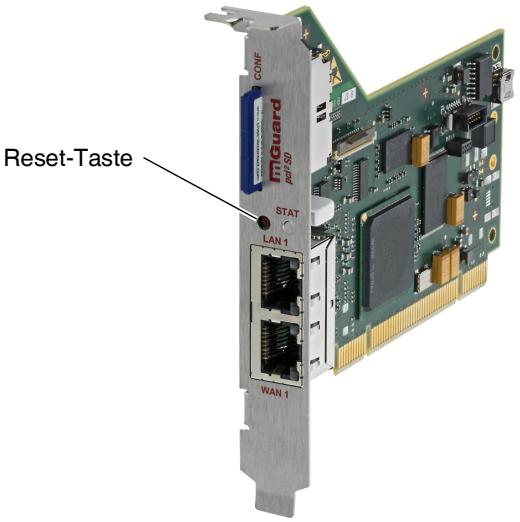


Bild 10-6 Reset-Taste

10.8.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Die Reset-Taste drücken, bis die LED STAT orange leuchtet.
- Alternativ den Computer, der die FL MGUARD PCI-Karte enthält, neu starten.

10.8.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 10-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät wird in den Stealth-Modus mit der Werkseinstellung „mehrere Clients“ zurückgesetzt.

– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
– Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Das Gerät befindet sich im Router- oder PPPoE-Modus.
– Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
– Sie kennen die aktuelle IP-Adresse des Geräts nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 10-6 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED STAT grün.
- Wenn die LED STAT erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED STAT grün
  Bei Misserfolg leuchtet die LED STAT rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

10.8.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ab mGuard-Firmwareversion 5.0.0 bleiben die im Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

- alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
- diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

- Alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
- Diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).
- Sie haben die Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
- Diese SD-Karte ist im Gerät eingesetzt.
- Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:
  Firmware/install-ubi.mpc83xx.p7s
  Firmware/ubifs.img.mpc83xx.p7s

Aktion

- Drücken Sie die Reset-Taste an der Frontblende und halten Sie sie gedrückt.
  Die LED STAT an der Frontblende leuchtet kurz orange.
  Anschließend leuchten die LED STAT sowie die LEDs der Ethernet- Buchsen (LAN1, LAN2, WAN1) nacheinander grün.
- Lassen Sie während der grünen Leuchtphase die Reset-Taste los.
  Die Flash-Prozedur startet.

10.9 Technische Daten

FL MGUARD PCI4000 | FL MGUARD PCI4000 VPN

Hardware-Eigenschaften		FL MGUARD PCI4000 | FL MGUARD PCI4000 VPN
Plattform		Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen		1 LAN-Port | 1 WAN-Port Ethernet IEEE 802.3 10/100 Base TX | RJ 45 | Full Duplex | Auto-MDIX
Sonstige Schnittstellen		seriell RS-232, interne Steckleiste
Speicher		128 MB RAM | 128 MB Flash SD-Karte, wechselbarer Konfigurationsspeicher
Laufwerke		–
Redundanz-Optionen		optional: VPN | Router
Stromversorgung		3,3 V oder 5 V, via PCI- (FL MGUARD PCI4000) oder PCI Express-Bus (FL MGUARD PCI4000 VPN)
Leistungsaufnahme		typisch 3,7 W ... 4,2 W
Luftfeuchtigkeitsbereich		5 % ... 95 % in Betrieb und Lagerung, nicht kondensierend
Schutzart		je nach Einbauart, abhängig vom Wirtssystem
Temperaturbereich	ohne Akku (HT-Variante)	0 °C ... +70 °C (Betrieb)
		-20 °C ... +70 °C (Lagerung)
	mit Akku	0 °C ... +60 °C (Betrieb)
		-20 °C ... +60 °C (Lagerung)
Maße (H x B x T)		95 mm x 18 mm x 130 mm
Gewicht		131 g
Gewicht (inkl. Verpackung)		200 g

Firmware und Leistungswerte	FL MGUARD PCI4000 | FL MGUARD PCI4000 VPN
Firmware-Kompatibilität	mGuard v7.5.0 oder höher; Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch Releases Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s
Hardware-basierte Verschlüsselung	DES | 3DES | AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 20 MBit/s
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software
Diagnose	LEDs (2 x LAN, 2 x WAN in Kombination) für Ethernet-Status und Geschwindigkeit; 1 LED für Power, Error, State, Fault, Info) | Log-File | Remote-Syslog

Sonstiges	FL MGUARD PCI4000 | FL MGUARD PCI4000 VPN
Konformität	CE | FCC
Besonderheiten	Echtzeituhr | Trusted Platform Module (TPM) | Temperatursensor | mGuard Remote Services Portal ready

11 FL MGUARD SMART2

Tabelle 11-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD SMART2	2700640
FL MGUARD SMART2 VPN	2700639

Produktbeschreibung

Der **FL MGUARD SMART2** ist die kleinste Geräteausführung. Er kann z. B. zwischen Rechner oder lokalem Netz und einem vorhandenem Router gesteckt werden, ohne dass beim bestehenden System Konfigurationsänderungen oder Treiberinstallationen erforderlich sind. Er ist konzipiert für den schnellen Einsatz im Büro oder unterwegs.

Bild 11-1 FL MGUARD SMART2

11.1 Bedienelemente und Anzeigen

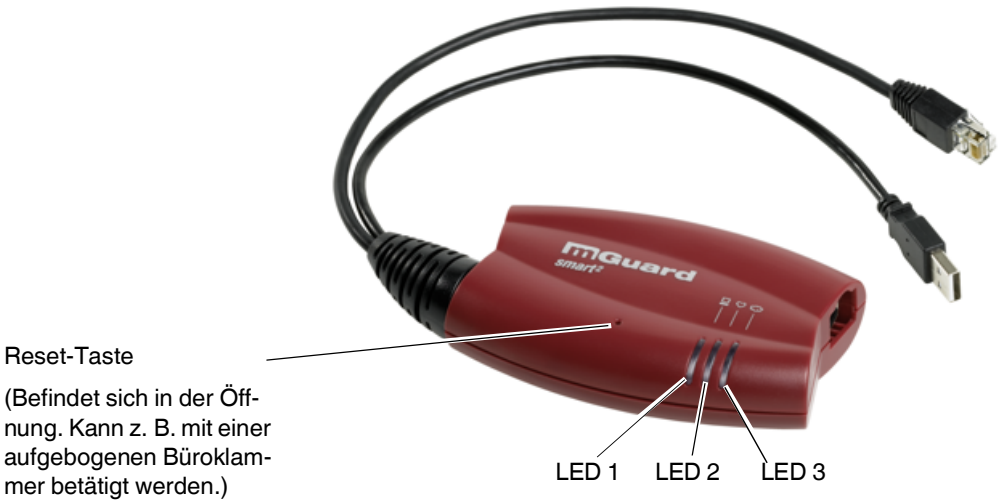


Bild 11-2 Bedienelemente und Anzeigen vom FL MGUARD SMART2

Tabelle 11-2 Anzeigen vom FL MGUARD SMART2

LED	Zustand		Bedeutung
1	Grün	Ein	LAN: Verbindung zum Netzwerk-Partner besteht
		Blinkt	LAN: Datenübertragung aktiv
2	Rot/Grün	Blinkt	**Bootvorgang**. Nach Anschluss des Gerätes an die Stromversorgungsquelle. Nach einigen Sekunden wechselt diese Anzeige zu Heartbeat.
	Grün	Blinkt	**Heartbeat**. Das Gerät ist korrekt angeschlossen und funktioniert.
	Rot	Blinkt	**Systemfehler**. Führen Sie einen Neustart durch. • Dazu die Reset-Taste kurz (1,5 Sek.) drücken. • Alternativ: das Gerät kurz von der Stromversorgung trennen und wieder anschließen. Falls der Fehler weiterhin auftritt, starten Sie die Recovery-Prozedur (siehe „Recovery-Prozedur ausführen“ auf Seite 231) oder wenden Sie sich an Ihren Händler.
3	Grün	Ein	WAN: Verbindung zum Netzwerk-Partner besteht
		Blinkt	WAN: Datenübertragung aktiv
1, 2, 3	Diverse LED-Leuchtcodes		**Recovery-Modus**. Nach Drücken der **Reset-Taste**. Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 230.

11.2 Inbetriebnahme

11.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

- Umgebungstemperatur:
  0 °C ... +40 °C
- Maximale Luftfeuchtigkeit, nicht kondensierend:
  20 % ... 90 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

11.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

- FL MGUARD SMART2
- Packungsbeilage

11.3 FL MGUARD SMART2 anschließen

LAN-Port

Ethernet-Stecker zum direkten Anschließen an das zu schützende Gerät bzw. Netz (**lokales** Gerät oder Netz).

USB-Stecker

Zum Anschließen an die USB-Schnittstelle eines Rechners.

Dient der Stromversorgung (Werkseinstellung).

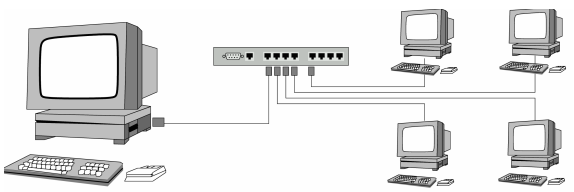
Der FL MGUARD SMART2 (nicht der FL MGUARD SMART) kann auch so konfiguriert werden, dass über den USB-Stecker eine serielle Konsole zur Verfügung steht.

WAN-Port

Buchse zum Anschließen an das externe Netzwerk, z. B. WAN, Internet. (Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)

Benutzen Sie ein UTP-Kabel (CAT5).

vorher:



nachher:

(Links kann auch ein LAN sein.)

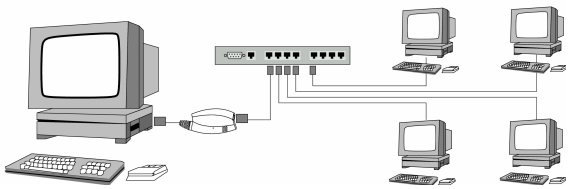


Bild 11-3 FL MGUARD SMART2: Anschuss im Netzwerk

Wenn Ihr Rechner bereits an einem Netzwerk angeschlossen ist, dann stecken Sie das Gerät zwischen die Netzwerkschnittstelle des Rechners (= dessen Netzwerkkarte) und das Netzwerk.

Es ist keine Treiber-Installation erforderlich.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

WARNUNG: Dies ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu treffen.

11.4 Konfiguration vorbereiten

11.4.1 Anschlussvoraussetzungen

- Das Gerät muss eingeschaltet sein, d. h. es muss per USB-Kabel an einen eingeschalteten Rechner (oder Netzteil) angeschlossen sein, so dass er mit Strom versorgt wird.
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss entweder
  - am LAN-Port des Geräts angeschlossen sein,
  - oder er muss über das lokale Netzwerk mit dem Gerät verbunden sein.
- **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

11.4.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS-Verfahren (Easy Initial Setup) eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen ohne Verbindung mit einem externen Netzwerk.

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 11-3 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät ist auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. Wenn Sie VPN-Verbindungen nutzen wollen, müssen Sie eine Management IP-Adresse und ein Standard-Gateway konfigurieren (siehe Seite 227). Alternativ können Sie eine andere Stealth-Konfiguration wählen oder einen anderen Netzwerk-Modus verwenden.

11.5 Konfiguration im Stealth-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter zwei IP-Adressen erreichbar:

– https://192.168.1.1/ (siehe Seite 225)
– https://1.1.1.1/ (siehe Seite 225)

Alternativ kann per BootP eine IP-Adresse zugewiesen werden (siehe „IP-Adresse per BootP zuweisen“ auf Seite 226).

Das Gerät ist unter der Adresse https://192.168.1.1/ erreichbar, wenn die externe Netzwerkschnittstelle beim Starten nicht verbunden ist.

Das Gerät kann von Rechnern über https://1.1.1.1/ erreicht werden, wenn diese direkt oder indirekt am LAN-Port des Geräts angeschlossen sind. Dazu muss das Gerät mit LAN- und WAN-Port in ein funktionierendes Netzwerk eingebunden sein, bei dem das Standard-Gateway über den WAN-Port erreichbar ist.

– Nach einem Zugriff über die IP-Adresse 192.168.1.1 und einer erfolgreichen Anmeldung wird die IP-Adresse 192.168.1.1 als Management IP-Adresse fest eingestellt.
– Nach einem Zugriff über die IP-Adresse 1.1.1.1 oder nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

11.5.1 IP-Adresse 192.168.1.1

Im Stealth-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.

- Das Gerät ist im Auslieferungszustand.
- Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
- Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

11.5.2 IP-Adresse https://1.1.1.1/

Bei konfigurierter Netzwerkschnittstelle

Damit das Gerät über die Adresse **https://1.1.1.1/** angesprochen werden kann, muss er an eine konfigurierte Netzwerkschnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt und dabei das Standard-Gateway über den WAN-Port des Geräts erreichbar ist.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des Geräts herstellen (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 227). Fahren Sie in diesem Falle dort fort.

Nach einem Zugriff über die IP-Adresse 1.1.1.1 steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

11.5.3 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

In Kapitel 14.1 wird die IP-Adressvergabe mit Hilfe der kostenlosen Windows-Software „IP Assignment Tool“ (IPAssign.exe) erklärt.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald das Gerät eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem das Gerät eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit das Gerät erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash) ausgeführt werden.

11.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgenden Adressen erreichbar:

Tabelle 11-4 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
FL MGUARD SMART2	Stealth	https://1.1.1.1/	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des Geräts vollständig ein (siehe Tabelle 11-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die IP-Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 231).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.
  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.
  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 11-4 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

11.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die IP-Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

11.8 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

Reset-Taste

(Befindet sich in der Öffnung. Kann z. B. mit einer aufgebogenen Büroklammer betätigt werden.)

Bild 11-5 Reset-Taste

11.8.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die mittlere LED in Rot aufleuchtet

  (Alternativ können Sie das USB-Kabel abziehen und aufstecken, da es ausschließlich zur Stromversorgung dient.)

11.8.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 11-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät wird in den Stealth-Modus mit der Werkseinstellung „mehrere Clients“ zurückgesetzt.

– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
– Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Das Gerät befindet sich im Router- oder PPPoE-Modus.
– Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 11-6 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die mittlere LED grün.
- Wenn die mittlere LED erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die mittlere LED grün.
  Bei Misserfolg leuchtet die mittlere LED rot.

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

11.8.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ab mGuard-Firmwareversion 5.0.0 bleiben die im Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

ACHTUNG: Zum Flashen der Firmware muss auf dem lokal angeschlossenen Rechner ein DHCP- und TFTP-Server oder ein BootP-und TFTP-Server installiert sein.

Installieren Sie den DHCP- und TFTP-Server, falls notwendig (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Aktion

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs grün leuchten.
  Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**
  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.
  Das Gerät startet nun das Rescue-System: Er sucht über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.
  Die mittlere LED blinkt.
  Vom TFTP-Server wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.
  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.
  Die drei grünen LEDs bilden ein Lauflicht.
  Vom TFTP-Server wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.
  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die mittlere LED leuchtet kontinuierlich.
  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.
- Sobald die Prozedur beendet ist, blinken alle drei LEDs gleichzeitig grün.
- Starten Sie das Gerät neu. Drücken Sie dazu kurz die **Reset-Taste**.
  Alternativ können Sie das USB-Kabel abziehen und aufstecken, da es ausschließlich zur Stromversorgung dient.

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie das mGuard-Gerät neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 227).

11.9 Technische Daten

Hardware-Eigenschaften	FL MGUARD SMART2
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN-Port | 1 WAN-Port Ethernet IEEE 802.3 10/100 Base TX | RJ 45 | Full Duplex | Auto-MDIX
Sonstige Schnittstellen	Seriell über USB-Anschluss
Laufwerke	–
Redundanz-Optionen	abhängig von der verwendeten Firmware
Stromversorgung	über USB Schnittstelle (5 V bei 500 mA) optional: externes Netzteil (110 V ... 230 V)
Leistungsaufnahme	max. 2,5 Watt
Temperaturbereich	0 °C ... +40 °C (Betrieb) -20 °C ... +60 °C (Lagerung)
Luftfeuchtigkeitsbereich	20 % ... 90 % in Betrieb, nicht kondensierend
Schutzart	IP30
Maße (H x B x T)	27 x 77 x 115 mm
Gewicht	185 g

Firmware und Leistungswerte	FL MGUARD SMART2
Firmware-Kompatibilität	mGuard v7.2 oder höher; Phoenix Contact empfiehlt Firmware die jeweils aktuellen Versionen in den jeweils aktuellen Patch Releases; Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s
Hardware-basierte Verschlüsselung	DES | 3DES | AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 20 MBit/s
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software
Diagnose	3 LEDs (in Kombination für Bootvorgang, Heartbeat, Systemfehler, Ethernet-Status, Recovery-Modus) | Log-File | Remote-Syslog

Sonstiges	FL MGUARD SMART2
Konformität	CE | FCC
Besonderheiten	Echtzeituhr | Trusted Platform Module (TPM) | Temperatursensor

12 FL MGUARD CENTERPORT

Tabelle 12-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD CENTERPORT	2702547

Produktbeschreibung

Der **FL MGUARD CENTERPORT** ist eine High-End-Firewall und ein VPN-Gateway im 19-Zoll-Format. Er ist als zentrale Netzwerkinfrastruktur für Remote-Service-Lösungen geeignet. Mit seinen Gigabit-Ethernet-Schnittstellen und dem entsprechendem Durchsatz als Router und als Stateful-Inspection-Firewall kann das Gerät auch im Backbone industrieller Netze eingesetzt werden.

Als Gateway unterstützt der FL MGUARD CENTERPORT die VPN-Anbindung beliebig vieler Systeme in VPN-Tunnel-Gruppen mit optional bis zu dreitausend gleichzeitig aktiven Tunneln, die alle zu einer einzigen öffentlichen IP-Adresse gehören.

Der FL MGUARD CENTERPORT leistet gesicherte Ferndienste wie Remote-Support, Ferndiagnose, Fernwartung und Condition-Monitoring für große Mengen von Maschinen und Anlagen über das Internet. Es ist ein verschlüsselter VPN-Datendurchsatz von 600 MBit/s an einem einzigen Interface möglich.

Der FL MGUARD CENTERPORT ist kompatibel mit allen mGuard-Feldgeräten und dem FL MGUARD DM. VPN-Lizenzen können bei Bedarf nachinstalliert werden.

Bild 12-1 FL MGUARD CENTERPORT

12.1 Bedienelemente und Anzeigen

Frontseite

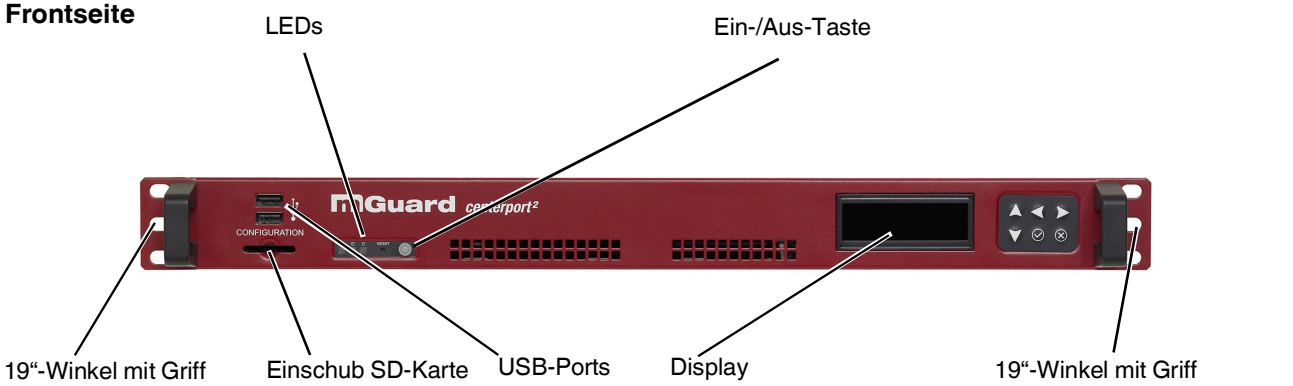


Bild 12-2 Bedienelemente und Anzeigen vom FL MGUARD CENTERPORT – Frontseite

Tabelle 12-2 Anzeigen vom FL MGUARD CENTERPORT

LED	Zustand	Bedeutung
Grün	Ein	Leuchtet, wenn das System eingeschaltet ist
Orange	Ein	Leuchtet, während Festplattenzugriff stattfindet

12.2 Inbetriebnahme

12.2.1 Sicherheitshinweise

Personal

Die Installation, Inbetriebnahme und Wartung des Produkts darf nur durch ausgebildetes und vom Betreiber autorisiertes Fachpersonal durchgeführt werden. Das Fachpersonal muss die Anweisungen in diesem Handbuch gelesen und verstanden haben und danach handeln.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

- Umgebungstemperatur:
  0 °C ... +45 °C
- Maximale Luftfeuchtigkeit, nicht kondensierend:
  20 % ... 90 %

Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Sachschaden durch Reinigungsmittel

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

12.2.2 Lieferumfang prüfen

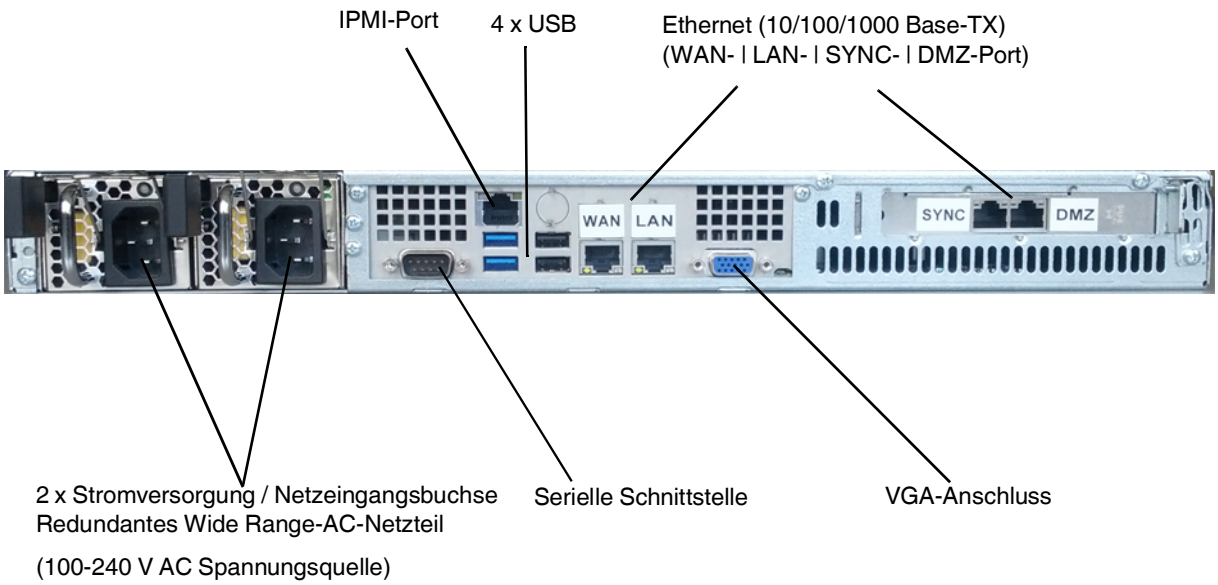
Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

- FL MGUARD CENTERPORT
- Packungsbeilage
- 2x AC-Netzanschlusskabel
- 19“-Serverschienen/Teleskopschienen (2x kurz, 2x lang)
- Schraubenset
- Einbauanleitung 19“-Rahmen/Industrieschrank (Quickrails Installation Instructions)

12.3 FL MGUARD CENTERPORT installieren und booten

Rückseite (Modell bis 2022)



Rückseite (Modell ab 2023)

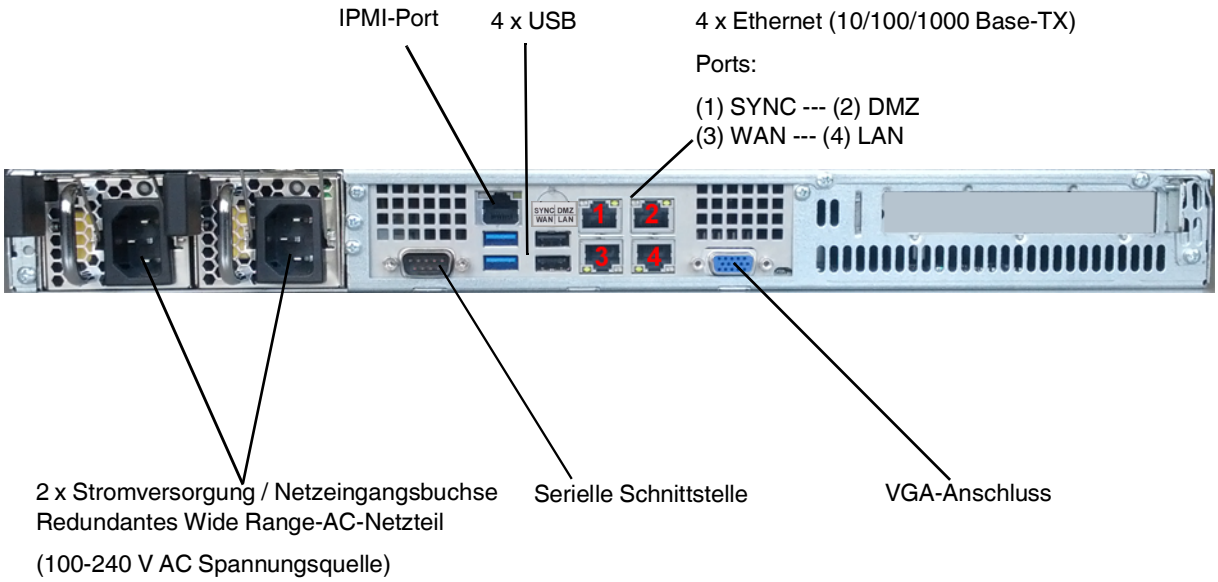


Bild 12-3 FL MGUARD CENTERPORT – Rückseite

12.3.1 Das Gerät anschließen

2. Optional: Bauen Sie das Gerät in einen 19"-Rahmen/Industrieschrank ein („Einbau in 19‘‘-Rahmen/Industrieschrank“ auf Seite 241).
3. Schließen Sie beide Netzeingangsbuchsen mittels Netzanschlusskabel am Netz bzw. an der Stromversorgungsquelle (100-240 V AC) an.

Damit der Zustand der Stromversorgung (Stromversorgung 1/2) im WBM korrekt angezeigt wird, muss die (redundante) Stromversorgung bereits **vor dem Anschalten des Gerätes** korrekt angeschlossen worden sein.

Ist dies nicht der Fall, müssen Sie das Gerät herunterfahren und die Stromversorgung für mindestens 30 Sekunden komplett vom Gerät trennen. Schließen Sie die Stromversorgung anschließend wieder korrekt an das Gerät an und starten Sie es neu.

4. Netzwerkverbindungen anschließen - siehe „Netzwerkverbindungen anschließen“ auf Seite 239.
5. Optional: Schließen Sie am VGA-Anschluss einen PC-Monitor an (nicht im Lieferumfang).
6. Optional: Schließen Sie an einem der USB-Anschlüsse eine PC-Tastatur an (nicht im Lieferumfang).

Tastatur und Monitor brauchen nicht angeschlossen sein, um das Gerät zu starten und zu betreiben. Bildschirm und Tastatur müssen nur angeschlossen werden,

- um beim Starten (Booten) vom FL MGUARD CENTERPORT eine der Boot-Optionen zu nutzen - siehe „Boot-Optionen - bei angeschlossenem Bildschirm und Tastatur“ auf Seite 241,
- um eine Rescue-Prozedur oder Recovery-Prozedur durchzuführen. Siehe „Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 247

12.3.2 Netzwerkverbindungen anschließen

WARNUNG: Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an.

Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

LAN-Port

- Benutzen Sie ein UTP-Kabel (CAT5).
- Verbinden Sie den LAN-Port des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des lokalen Konfigurationsrechners oder einem Netzwerkanschluss des lokalen Netzwerks (LAN).

WAN-Port

- Benutzen Sie ein UTP-Kabel (CAT5).
- Verbinden Sie den WAN-Port des Geräts mit dem externen Netzwerk bzw. Internet. (Über dieses Netz werden die Verbindungen zum entfernten Gerät bzw. Netz hergestellt.)

SYNC-Port

- Benutzen Sie ein UTP-Kabel (CAT5).

- Verbinden Sie den SYNC-Port des Geräts mit dem SYNC-Port eines zweiten FL MGUARD CENTERPORT, um ein Redundanzpaar zu bilden. Eine Redundanzlizenz für den zweiten FL MGUARD CENTERPORT muss separat erworben werden.

DMZ-Port

- Benutzen Sie ein UTP-Kabel (CAT5).
- Verbinden Sie den DMZ-Port des Geräts mit einem Netzwerkanschluss des lokalen Netzwerkes (LAN). Über dieses Netz wird entsprechend den Firewall-Regeln der Demilitarisierten Zone (DMZ) kommuniziert.

IPMI-Port

- Benutzen Sie ein UTP-Kabel (CAT5).

Der **IPMI-Port** ist standardmäßig deaktiviert und wird an dieser Stelle nicht dokumentiert. Die Funktionen des IPMI-Ports lassen sich im BIOS-Setup des Motherboards aktivieren. Bei Fragen zur Dokumentation wenden Sie sich bitte an den Hersteller Super Micro Computer, Inc. (http://www.supermicro.com).

Serielle Schnittstelle

ACHTUNG: Die serielle Schnittstelle (D-SUB-Buchse) darf nicht direkt mit Fernmeldeanschlüssen verbunden werden. Zum Anschluss eines seriellen Terminals oder eines Modems ist ein serielles Kabel mit D-SUB-Stecker zu verwenden. Die maximale Leitungslänge des seriellen Kabels beträgt 30 m.

Die serielle Schnittstelle kann wie folgt verwendet werden:

Zum **Konfigurieren des Geräts** über die serielle Schnittstelle. Dazu gibt es zwei Möglichkeiten:

– An die serielle Schnittstelle des Geräts wird direkt ein PC angeschlossen (über dessen serielle Schnittstelle). Dann kann der PC-Benutzer mittels eines Terminalprogramms über die Kommandozeile das Gerät konfigurieren.
– Oder an die serielle Schnittstelle des Geräts wird ein Modem angeschlossen, das am Telefonnetz (Festnetz oder GSM-Netz) angeschlossen ist. Dann kann der Benutzer eines entfernten PCs, der ebenfalls mit einem Modem am Telefonnetz angeschlossen ist, zum Gerät eine PPP-Wählverbindung (PPP = Point-to-Point Protocol) herstellen und ihn per Web-Browser konfigurieren.

Zur **Abwicklung des Datenverkehrs** statt über die WAN-Schnittstelle des Geräts über die serielle Schnittstelle. In diesem Fall ist an die serielle Schnittstelle ein Modem anzuschließen.

12.3.3 Einbau in 19‘‘-Rahmen/Industrieschrank

Die Netzanschlusskabel der Netzteile werden als Netztrennstelle genutzt. Deshalb müssen für die Netzstecker leicht zugängliche Steckdosen nahe dem Gerät verwendet werden. Um das Gerät vom Netz zu trennen, müssen die Netzstecker gezogen werden. Falls das Gerät in einen Schaltschrank mit nicht zugänglichen Steckdosen eingebaut wird, muss bei der Installation eine geeignete Trennvorrichtung vom Netz installiert werden (z. B. ein zugelassener Trennschalter).

Eine ausreichende Luftzirkulation muss sichergestellt werden. Bei einer Stapelung von mehreren FL MGUARD CENTERPORT müssen ein oder mehrere 19"-Lüftereinschübe vorgesehen werden, damit die aufgestaute Warmluft abgeführt werden kann. Die verwendeten Schaltschränke müssen den Anforderungen an Brandschutzgehäuse und mechanischen Schutz nach EN60950-1 entsprechen.

Informationen zum Einbau eines FL MGUARD CENTERPORT entnehmen Sie bitte der dem Gerät beiliegenden Einbauanleitung „Quickrails Installation Instructions“.

12.3.4 FL MGUARD CENTERPORT starten (booten)

- Schalten Sie das Gerät durch drücken der Ein-/Aus-Taste ein.
- Nach dem Einschalten des Geräts leuchtet die Statusanzeige LED (grün). Eine weitere LED (orange) leuchtet bei jedem Festspeicherzugriff.
- Das Gerät bootet die Firmware und ist betriebsbereit.
- Das Display zeigt Statusmeldungen der mGuard-Firmware an.

12.3.4.1 Boot-Optionen - bei angeschlossenem Bildschirm und Tastatur

Wenn ein Bildschirm und eine Tastatur am Gerät angeschlossen sind, gibt es folgende Optionen:

– Nach dem Einschalten,
– oder nach einem Neustart

werden auf dem Bildschirm zunächst die Boot-Meldungen des BIOS angezeigt.

Soll das Boot-Menü angezeigt werden, drücken Sie auf der Tastatur mehrmals eine der Richtungstasten: ↑, ↓, ← oder →.

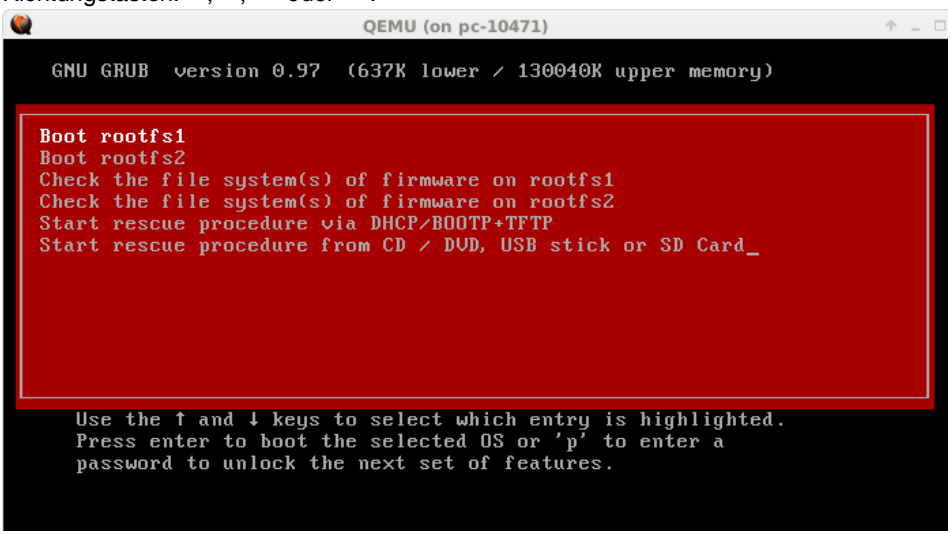


Bild 12-4 Boot-Menü des FL MGUARD CENTERPORT

Zum Auswählen und Inkraftsetzen einer der Boot-Optionen wie folgt vorgehen:

1. Mit den Richtungstasten ↓ bzw. ↑ eine der angezeigten Optionen auswählen.
2. Dann die **Enter-**Taste drücken.

Boot-Optionen

Boot rootfs1

Starten der primären auf dem Gerät befindlichen Firmware-Version „A“. Das ist die Standardeinstellung: Sie tritt in Kraft, wenn der Benutzer beim Starten nicht eingreift.

Boot rootfs2

Wird von der aktuellen Firmware-Version nicht unterstützt.

Check the file system(s) of firmware on rootfs1

Überprüft und repariert gegebenenfalls alle Dateisysteme der Firmware.
Dieser Menüpunkt braucht nur im besonderen Bedarfsfall bei entsprechender Kenntnis des Benutzers oder auf Anweisung des Supports Ihres Händlers verwendet werden. Die Firmware des Geräts überprüft und repariert die Dateisysteme bei Bedarf auch während des normalen Startvorganges. Die Firmware verwendet ihre Dateisysteme in sehr robuster Weise bei ausgeschaltetem Cache des Massenspeichermediums, so dass in der Regel kein Reparaturbedarf entsteht.

Check the file system(s) of firmware on rootfs2

Wird von der aktuellen Firmware-Version nicht unterstützt.

Start rescue procedure via DHCP/BootP+TFTP
Start rescue procedure from CD / DVD, USB stick or SD Card

„Neustart, Recovery-Prozedur und Flashen der Firmware“ auf Seite 247

12.4 Konfiguration vorbereiten

12.4.1 Anschlussvoraussetzungen

- Beim Gerät müssen beide Netzteile an der Stromversorgungsquelle/am Netz angeschlossen sein. (Wenn nur ein Netzteil angeschlossen ist, kann das Gerät zwar betrieben werden, aber es wird ein akustisches Signal ausgegeben.)
- **Bei lokaler Konfiguration:** Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an den LAN-Port des Geräts angeschlossen sein.
- **Bei Fernkonfiguration:** Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

12.4.2 Lokale Konfiguration bei Inbetriebnahme (Router-Modus)

Bei Auslieferung oder nach Zurücksetzen auf die Werkseinstellung oder Flashen des Geräts ist das Gerät über die LAN Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar.

Für einen Zugriff auf die Konfigurationsoberfläche kann es daher nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Beispiel

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

12.5 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgenden Adressen erreichbar:

Tabelle 12-3 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
FL MGUARD CENTERPORT	Router	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen HTTPS-fähigen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des Geräts vollständig ein (siehe Tabelle 12-3).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 247).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.
  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.
  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.
  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.
  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis grundsätzlich mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 12-5 Login

Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

12.6 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die IP-Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

12.7 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

12.8 Neustart, Recovery-Prozedur und Flashen der Firmware

Um eine Recovery-Prozedur oder das Flashen der Firmware durchzuführen, muss das Gerät neu gestartet werden.

12.8.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Ein-/Aus-Taste des gestarteten Geräts ca. 5 s lang, um das Gerät auszuschalten. (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)
- Anschließend drücken Sie die Ein-/Aus-Taste erneut kurz, um das Gerät neu zu starten.

12.8.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 12-4 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Das Gerät wird in den Router-Modus mit fester IP-Adresse zurückgesetzt.

– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
– Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

ACHTUNG: Nach erfolgreich ausgeführter Recovery-Prozedur sollte ein zuvor erstelltes Konfigurationsprofil im Gerät neu geladen und aktiviert werden. Anschließend sollten die Netzwerkeinstellungen angepasst werden.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Das Gerät befindet sich im PPPoE-Modus.
– Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.

– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. (Application Notes stehen im Download-Bereich von phoenixcontact.net/products bereit.)

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 12-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1 (IP-Adresse der internen Schnittstelle)
Router	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

Voraussetzung: Am Gerät sind Bildschirm und Tastatur angeschlossen.

- Auf der Tastatur die folgende Tastenkombination drücken: <**Alt**>+<**S-Abf**>+<**a**>.

(Auf englischen Tastaturen ist die oben mit <**S-Abf>** bezeichnete Taste mit <**SysRq**> beschriftet. Auf manchen Tastaturen fehlt aber die Beschriftung <**S-Abf**> bzw. <**SysRq**>. Dann ist die Taste <**Druck**> bzw. <**Print**> zu verwenden.)

Nach einmaligem Drücken der Tastenkombination muss die gleiche Kombination innerhalb von 30 s erneut gedrückt werden, um die Recovery-Prozedur zu starten.

Nach erfolgreicher Ausführung der Recovery-Prozedur erscheint auf dem Bildschirm eine entsprechende Meldung.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

12.8.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis FL/TC MGUARD-Geräte updaten und flashen, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ab mGuard-Firmwareversion 5.0.0 bleiben die im Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Das Flashen der Firmware kann auf drei Wegen erfolgen:

- via Netzwerk (TFTP- und DHCP-Server)
- via USB-Anschluss (USB-Flash-Laufwerk oder USB-CD/DVD-Laufwerk)
- via SD-Speicherkarte

Voraussetzung für das Laden der Firmware von einer **SD-Karte**, einem **USB-Flash-Laufwerk**:

- Beachten Sie, dass die Funktionalität der SD-Karte und des Produktes nur bei Einsatz einer Phoenix Contact SD-Karte (z. B. SD FLASH 2GB - 2988162) sichergestellt werden kann.
- Alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte bzw. des USB-Flashspeichers unter folgendem Pfadnamen bzw. in folgendem Ordner vorliegen:
  /Firmware/install.x86_64.p7s
  /Firmware/firmware.img.x86_64.p7s

Voraussetzung für das Laden der Firmware von einem **TFTP-Server**:

- Ein TFTP-Server muss auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

- Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden **Firmware-Dateien** zum Herunterladen bereit.

Vorbereitung

- Sie haben die Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf dem Installationsmedium Ihrer Wahl bzw. dem lokalen Installationsrechner gespeichert.
- Falls die Ihnen vorliegende Firmware-Version höher ist als die beim Auslieferungszustand des Gerätes, müssen Sie eine Lizenz für die Nutzung dieses Updates erwerben. Das gilt für Major-Release Upgrades, also z. B. beim Upgrade von Version 6.x.y zu Version 7.x.y zu Version 8.x.y usw.
- **Option SD-Karte:** Die SD-Karte ist im Gerät eingesetzt.
- **Option USB-Anschluss:** Ein USB-Flash-Laufwerk oder eine USB-CD/DVD-Laufwerk ist an den USB-Port des Geräts angeschlossen.
- **Option Netzwerk:** DHCP- und TFTP-Server sind unter der gleichen IP-Adresse zu erreichen.

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Alle konfigurierten Einstellungen werden gelöscht.

Das Gerät wird in den Auslieferungszustand versetzt.

Ab mGuard-Firmwareversion 5.0.0 des mGuard bleiben die im mGuard installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

1. Gerät neu starten/booten.
2. Sobald das Gerät bootet, drücken Sie auf der Tastatur mehrmals eine der Pfeiltasten: ↑, ↓, ← oder → bis der Bootvorgang unterbrochen wird.
3. Das Boot-Menü wird angezeigt.

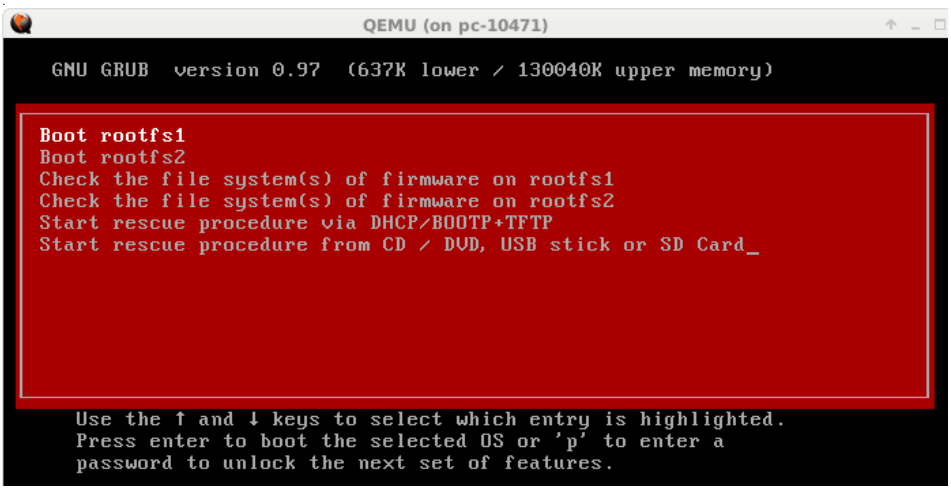


Bild 12-6 Boot-Menü – FL MGUARD CENTERPORT

4. Wählen Sie mit den Pfeiltasten ↓ bzw. ↑ eine der Optionen zur Durchführung der Rescue-Prozedur aus:
   Start rescue procedure via DHCP / BOOTP+TFTP
   ODER
   Start rescue procedure from CD / DVD, USB stick or SD Card
   Zum Inkraftsetzen der Auswahl die **Enter**-Taste drücken.
   Die Optionen beinhalten:

Start rescue procedure via DHCP / BootP+TFTP

Wirkung: Das Gerät lädt die notwendigen Dateien vom TFTP-Server:

– install.x86_64.p7s
– firmware.img.x86_64.p7s

Start rescue procedure from CD/DVD, USB stick or SD Card

Allgemeine Voraussetzungen:

1. Ein an den USB-Port angeschlossenes CD/DVD-Laufwerk oder
2. ein an den USB-Port angeschlossener USB stick (USB-Flash-Laufwerk) oder
3. eine in das SD-Card-Laufwerk eingesetzte SD-Speicherkarte.

Nach dem Starten des Rescue-Prozedur durch drücken der Enter-Taste werden die notwendigen Daten von dem Medium geladen, das an das Gerät angeschlossen bzw. eingesetzt wurde.

Start rescue procedure from CD/DVD

Voraussetzung: Die Firmware des Geräts ist zuvor auf eine CD/DVD gebrannt worden - siehe unten unter „mGuard-Firmware auf CD/DVD-ROM brennen“ auf Seite 252.

Wirkung: Das Gerät lädt alle notwendigen Dateien von der eingelegten CD/DVD.

Legen Sie während der Anzeige des Boot-Menüs und vor Inkraftsetzen dieser Auswahl die CD/DVD mit der Firmware des Geräts in das CD/DVD-Laufwerk ein. (Aus Sicherheitsgründen bootet der FL MGUARD CENTERPORT nicht von CD/DVD.)

– Nach der Rescue-Prozedur erscheint auf dem Bildschirm eine entsprechende Meldung. Folgen Sie möglichen weiteren Anweisungen auf dem Bildschirm.

Start rescue procedure from USB stick (USB-Flash-Laufwerk)

Voraussetzung: Die Firmware des Gerät ist zuvor auf ein USB-Speichermedium (USB-Stick, USB-Flash-Laufwerk) kopiert worden:

/Firmware/install.x86_64.p7s

/Firmware/firmware.img.x86_64.p7s

Wirkung: Das Gerät lädt alle notwendigen Dateien vom angeschlossenen USB-Speichermedium. (Aus Sicherheitsgründen bootet der FL MGUARD CENTERPORT nicht vom USB-Speichermedium.)

– Nach der Rescue-Prozedur erscheint auf dem Bildschirm eine entsprechende Meldung. Folgen Sie möglichen weiteren Anweisungen auf dem Bildschirm.

Start rescue procedure from SD Card

Voraussetzung: Die Firmware des Geräts ist zuvor auf die SD-Karte kopiert worden:
/Firmware/install.x86_64.p7s
/Firmware/firmware.img.x86_64.p7s
Wirkung: Das Gerät lädt alle notwendigen Dateien von der eingesetzten SD-Karte. Setzen Sie dazu spätestens während der Anzeige des Boot-Menüs und vor Inkraftsetzen dieser Auswahl die SD-Karte mit der gespeicherten Firmware in das Gerät ein. (Aus Sicherheitsgründen bootet der FL MGUARD CENTERPORT nicht von einer SD-Karte.)

– Nach der Rescue-Prozedur erscheint auf dem Bildschirm eine entsprechende Meldung. Folgen Sie möglichen weiteren Anweisungen auf dem Bildschirm.

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie das mGuard-Gerät neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 244):

mGuard-Firmware auf CD/DVD-ROM brennen

Die Firmware des Geräts kann auf CD/DVD gebrannt werden. Auf der Download-Seite phoenixcontact.net/products steht dazu eine zip-Datei zum Herunterladen bereit.

Brennen Sie den Inhalt dieses zip-Archivs als Daten-CD/DVD. Auf der CD/DVD müssen die folgenden Dateien in folgenden Ordnern bzw. unter folgenden Pfadnamen liegen:

– /Firmware/install.x86_64.p7s
– /Firmware/firmware.img.x86_64.p7s

12.9 Technische Daten

Hardware-Eigenschaften	FL MGUARD CENTERPORT
Plattform	Multi-Core x86 Prozessorarchitektur
Netzwerk Schnittstellen	1 LAN-Port | 1 WAN-Port | 1 SYNC-Port | 1 DMZ-Port Ethernet IEEE 802.3 10/100/1000 Base TX | RJ 45 | Full/Half Duplex | Auto-MDIX
Sonstige Schnittstellen	VGA-Konsole | seriell RS-232, D-SUB 9-Stecker | 6 x USB
Laufwerke	1 HDD | 1 SD-Card
Redundanz-Optionen	optionale Lizenz VPN | Router & Firewall
Stromversorgung	2 x 100 V AC ... 240 V AC, 300 W bei 50/60 Hz, redundant
Leistungsaufnahme	abhängig von der jeweiligen Ausbaustufe
Luftfeuchtigkeitsbereich	20 % ... 90 % in Betrieb, nicht kondensierend 10 % ... 90 % außer Betrieb
Schutzart	Front IP 20
Temperaturbereich	0 °C ... +45 °C (Betrieb) -20 °C ... +70 °C (Lagerung)
Maße (H x B x T)	44 x 447 x 458 mm (1 U x 19“ x 18.5“)
Gewicht	17 kg

Firmware und Leistungswerte	FL MGUARD CENTERPORT
Firmware-Kompatibilität	mGuard v8.1.2 oder höher; Phoenix Contact empfiehlt den Einsatz in den jeweils aktuellen Patch-Releases. Funktionsumfang siehe entsprechendes Firmware-Datenblatt bzw. die entsprechenden Release Notes.
Datendurchsatz (Router | Firewall)	2.000 Mbit/s bidirektional | 2.000 Mbit/s bidirektional Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.
Hardware-basierte Verschlüsselung	DES | 3DES | AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	600 Mbit/s bidirektional (Router-Modus) Bei Nutzung der DMZ als eigenständige Netzwerkzone wird der maximal mögliche Durchsatz auf die drei Zonen aufgeteilt.
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software
Diagnose	Dot-Matrix-Display | LEDs | Boot-Menü | Log-File | Remote-Syslog

Sonstiges	FL MGUARD CENTERPORT
Konformität	FCC, CE, entwickelt nach UL-Anforderungen

13 FL MGUARD DELTA TX/TX

Tabelle 13-1 Aktuell verfügbare Produkte

Produktbezeichnung	Phoenix Contact Artikelnummer
FL MGUARD DELTA TX/TX	2700967
FL MGUARD DELTA TX/TX VPN	2700968

Produktbeschreibung

Der **FL MGUARD DELTA TX/TX** ist prädestiniert für den Einsatz im Desktop-Bereich, in Verteilerräumen, Netzwerkschränken und anderen produktionsnahen Umgebungen mit geringen Anforderungen an eine industrielle Härtung.

Einzelteilnehmer oder Netzwerksegmente können sicher vernetzt und umfassend geschützt werden. Der FL MGUARD DELTA TX/TX eignet sich als Firewall zwischen Büro- und Produktionsnetzen sowie als Security-Router für kleine und mittlere Arbeitsgruppen.

Bild 13-1 FL MGUARD DELTA TX/TX

13.1 Bedienelemente und Anzeigen

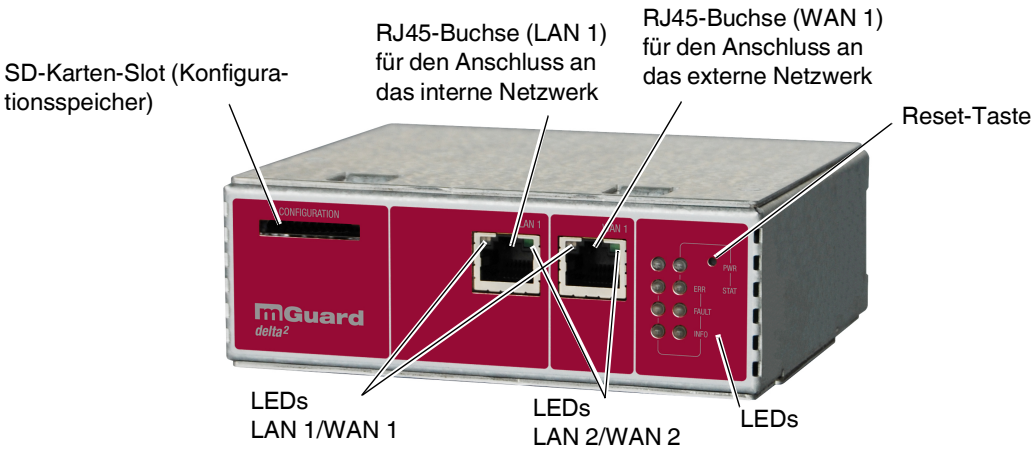


Bild 13-2 Bedienelemente und Anzeigen vom FL MGUARD DELTA TX/TX

Tabelle 13-2 Anzeigen vom FL MGUARD DELTA TX/TX

LEDs	Zustand		Bedeutung
WAN 1	Grün	Ein	Vollduplex
LAN 1		Aus	Halbduplex
WAN 2	Gelb	Ein	10 MBit/s
LAN 2		Blinkt	10 MBit/s, Datenübertragung aktiv
	Grün	Ein	100 MBit/s
		Blinkt	100 MBit/s, Datenübertragung aktiv
PWR	Grün	Ein	Versorgungsspannung o.k.
STAT	Grün	Blinkt	Das Gerät ist betriebsbereit.
ERR	Rot	Ein	Systemfehler
FAULT	Rot	Ein	Das Gerät ist im Zustand Booten oder Flashen
INFO			Nicht belegt

13.2 Inbetriebnahme

13.2.1 Sicherheitshinweise

Um den ordnungsgemäßen Betrieb sicherzustellen und die Sicherheit der Umgebung und von Personen zu gewährleisten, muss das Gerät richtig installiert, betrieben und gewartet werden.

ACHTUNG: Sachschaden durch falsche Beschaltung

Schließen Sie die Netzwerk-Ports des Geräts nur an LAN-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen, diese dürfen nicht mit den RJ45-Buchsen des Geräts verbunden werden.

Allgemeine Hinweise zur Benutzung

ACHTUNG: Umgebungsbedingungen passend auswählen

- Umgebungstemperatur:
  0 °C ... +40 °C
- Maximale Luftfeuchtigkeit, nicht kondensierend:
  5 % ... 95 %
  Setzen Sie das Gerät keinem direktem Sonnenlicht oder dem direkten Einfluss einer Wärmequelle aus, um eine Überhitzung zu vermeiden.

ACHTUNG: Reinigen

Verwenden Sie zum Reinigen des Gerätegehäuses ein weiches Tuch. Verwenden Sie keine aggressiven Lösungsmittel.

13.2.2 Lieferumfang prüfen

Prüfen Sie die Lieferung vor der Inbetriebnahme auf Vollständigkeit.

Zum Lieferumfang gehören

- FL MGUARD DELTA TX/TX
- Packungsbeilage
- eine 12 V DC-Stromversorgung inkl. diverser Länder-Adapter

13.3 FL MGUARD DELTA TX/TX anschließen

ACHTUNG: Hinweise zu Montage und Installation

Schließen Sie die RJ45-Ethernet-Ports des Geräts nur an passende Netzwerk-Installationen an. Einige Fernmeldeanschlüsse verwenden ebenfalls RJ45-Buchsen. Diese dürfen Sie nicht mit den RJ45-Anschlüssen des Geräts verbinden.

Die sichere Trennung von berührungsgefährlichen Stromkreisen ist nur gewährleistet, wenn die angeschlossenen Geräte die Anforderungen der VDE 0106-101 (Sichere Trennung) erfüllen. Für die sichere Trennung sind die Zuleitungen getrennt von berührungsgefährlichen Stromkreisen zu führen oder zusätzlich zu isolieren.

13.3.1 Mit dem Netzwerk verbinden

- Verbinden Sie das Gerät mit dem Netzwerk. Dazu benötigen Sie ein geeignetes UTP-Kabel (CAT5), das nicht zum Lieferumfang gehört.
- Verbinden Sie die interne Netzwerkschnittstelle LAN 1 des Geräts mit der entsprechenden Ethernet-Netzwerkkarte des Konfigurationsrechners oder einem validen Netzwerk-Anschluss des internen Netzwerks (LAN).

13.3.2 Versorgungsspannung anschließen

- Verbinden Sie das Weitbereichs-Netzteil des Geräts mit einer geeigneten Stromversorgung. Schließen Sie den Niederspannungs-Stecker des Netzteils auf der Rückseite des Geräts an.

Bild 13-3 Niederspannungs-Stecker des Netzteils

Die Status-Anzeige PWR leuchtet grün, wenn die Versorgungsspannung korrekt angeschlossen ist.

Das Gerät bootet die Firmware. Die Status-Anzeige STAT blinkt grün.

Das Gerät ist betriebsbereit, sobald die LAN/WAN-LEDs der Ethernet-Buchsen leuchten.

Zusätzlich leuchten die Status-Anzeigen PWR grün und die Status-Anzeige STAT blinkt grün im Heartbeat.

13.4 Konfiguration vorbereiten

13.4.1 Anschlussvoraussetzungen

FL MGUARD DELTA TX/TX

- Das Gerät muss an seine Stromversorgung angeschlossen sein.
- **Bei lokaler Konfiguration**: Der Rechner, mit dem Sie die Konfiguration vornehmen, muss an der LAN-Buchse des Geräts angeschlossen sein.
- **Bei Fernkonfiguration**: Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.
- Das Gerät muss angeschlossen sein, d. h. die erforderlichen Verbindungen müssen funktionieren.

13.4.2 Lokale Konfiguration bei Inbetriebnahme (EIS)

Die Erstinbetriebnahme von mGuard-Produkten, die im Stealth-Modus ausgeliefert werden, ist ab der Firmware-Version 7.2 deutlich vereinfacht worden. Ab dieser Version ermöglicht das EIS-Verfahren (Easy Initial Setup) eine Inbetriebnahme über voreingestellte oder benutzerdefinierte Management-Adressen ohne Verbindung mit einem externen Netzwerk.

Das Gerät wird per Web-Browser konfiguriert, der auf dem zum Konfigurieren verwendeten Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist nach Werkseinstellung unter folgenden Adressen erreichbar:

Tabelle 13-3 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät ist auf die Stealth-Konfiguration „mehrere Clients“ voreingestellt. Wenn Sie VPN-Verbindungen nutzen wollen, müssen Sie eine Management IP-Adresse und ein Standard-Gateway konfigurieren (in der Web-Oberfläche unter „Netzwerk >> Interfaces >> Allgemein“). Alternativ können Sie eine andere Stealth-Konfiguration wählen oder einen anderen Netzwerk-Modus verwenden.

13.5 Konfiguration im Stealth-Modus

Bei der ersten Inbetriebnahme ist das Gerät unter zwei IP-Adressen erreichbar:

– https://192.168.1.1/ (siehe Seite 261)
– https://1.1.1.1/ (siehe Seite 261)

Alternativ kann per BootP eine IP-Adresse zugewiesen werden (siehe „IP-Adresse per BootP zuweisen“ auf Seite 262).

Das Gerät ist unter der IP-Adresse https://192.168.1.1/ erreichbar, wenn die externe Netzwerkschnittstelle beim Starten nicht verbunden ist.

Das Gerät kann von Rechnern über https://1.1.1.1/ erreicht werden, wenn diese direkt oder indirekt am LAN-Port des Geräts angeschlossen sind. Dazu muss das Gerät mit LAN- und WAN-Port in ein funktionierendes Netzwerk eingebunden sein, bei dem das Standard-Gateway über den WAN-Port erreichbar ist.

– Nach einem Zugriff über die IP-Adresse 192.168.1.1 und einer erfolgreichen Anmeldung wird die IP-Adresse 192.168.1.1 als Management IP-Adresse fest eingestellt.
– Nach einem Zugriff über die IP-Adresse 1.1.1.1 oder nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

13.5.1 IP-Adresse 192.168.1.1

Im Stealth-Modus ist das Gerät über die LAN-Schnittstelle unter der IP-Adresse 192.168.1.1 innerhalb des Netzwerks 192.168.1.0/24 erreichbar, wenn eine dieser Bedingungen zutrifft.

- Das Gerät ist im Auslieferungszustand.
- Das Gerät wurde über die Web-Oberfläche auf die Werkseinstellung zurückgesetzt und neu gestartet.
- Die Rescue-Prozedur (Flashen des Geräts) oder die Recovery-Prozedur wurden ausgeführt.

Für einen Zugriff auf die Konfigurationsoberfläche kann es nötig sein, die Netzwerk-Konfiguration Ihres Computers anzupassen.

Unter **Windows 7** gehen Sie dazu wie folgt vor:

- Öffnen Sie in der Systemsteuerung das „Netzwerk und Freigabecenter“.
- Klicken Sie auf „LAN-Verbindung“. (Der Punkt „LAN-Verbindung" wird nur angezeigt, wenn eine Verbindung von der LAN-Schnittstelle des Rechners zu einem mGuard-Gerät in Betrieb oder einer anderen Gegenstelle besteht.)
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Wählen Sie den Auswahlpunkt „Internetprotokoll Version 4 (TCP/IPv4)“ aus.
- Klicken Sie auf die Schaltfläche „Eigenschaften“.
- Aktivieren Sie unter „Eigenschaften von Internetprotokoll Version 4“ zunächst „Folgende IP-Adresse verwenden“ und geben dann zum Beispiel folgende Adresse ein:

IP-Adresse:	192.168.1.2
Subnetzmaske:	255.255.255.0
Standard-Gateway:	192.168.1.1

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

13.5.2 IP-Adresse https://1.1.1.1/

Bei konfigurierter Netzwerkschnittstelle

Damit das Gerät über die Adresse **https://1.1.1.1/** angesprochen werden kann, muss er an eine konfigurierte Netzwerkschnittstelle angeschlossen sein. Das ist der Fall, wenn man ihn zwischen eine bestehende Netzwerkverbindung steckt und dabei das Standard-Gateway über den WAN-Port des Geräts erreichbar ist.

In diesem Fall wird der Web-Browser nach Eingabe der Adresse https://1.1.1.1/ die Verbindung zur Konfigurations-Oberfläche des Geräts herstellen (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 263). Fahren Sie in diesem Falle dort fort.

Nach einem Zugriff über die IP-Adresse 1.1.1.1 steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

13.5.3 IP-Adresse per BootP zuweisen

Nach der Zuweisung einer IP-Adresse per BootP steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Für die IP-Adressvergabe nutzt das Gerät das BootP-Protokoll. Sie können die IP-Adresse auch über BootP zuweisen. Das Internet stellt eine Vielzahl von BootP-Servern zur Verfügung. Sie können ein beliebiges dieser Programme für die Adressvergabe nutzen.

In Kapitel 14.1 wird die IP-Adressvergabe mit Hilfe der kostenlosen Windows-Software „IP Assignment Tool“ (IPAssign.exe) erklärt.

Hinweise zu BootP

Bei der ersten Inbetriebnahme sendet das Gerät ununterbrochen bis zum Erhalt einer gültigen IP-Adresse BootP-Requests aus. Sobald das Gerät eine korrekte IP-Adresse erhält, werden keine weiteren BootP-Requests gesendet. Danach steht die IP-Adresse 192.168.1.1 nicht länger als Zugriffsmöglichkeit zur Verfügung.

Nachdem das Gerät eine BootP-Antwort erhalten hat, sendet er keine BootP-Anfragen aus, auch nicht nach einem Neustart. Damit das Gerät erneut BootP-Requests sendet, muss entweder die Werkseinstellung wiederhergestellt oder eine der Prozeduren (Recovery oder Flash) ausgeführt werden.

13.6 Lokale Konfigurationsverbindung herstellen

Web-basierte Administratoroberfläche

Das Gerät wird per Web-Browser konfiguriert, der auf dem Konfigurations-Rechner ausgeführt wird.

ACHTUNG: Der verwendete Web-Browser muss SSL-Verschlüsselung (d. h. HTTPS) unterstützen.

Das Gerät ist unter einer der folgenden Adressen erreichbar::

Tabelle 13-4 Voreingestellte Adressen

Werkseinstellung	Netzwerk-Modus	Management-IP #1	Management-IP #2
FL MGUARD DELTA TX/TX	Stealth	https://1.1.1.1/	https://192.168.1.1/

Gehen Sie wie folgt vor:

- Starten Sie einen Web-Browser.
- Achten Sie darauf, dass der Browser beim Starten nicht automatisch eine Verbindung wählt, weil sonst die Verbindungsaufnahme zum Gerät erschwert werden könnte.

Im **Internet Explorer** nehmen Sie diese Einstellung wie folgt vor:

- Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“:
- Unter „DFÜ- und VPN-Einstellungen“ muss „Keine Verbindung wählen“ aktiviert sein.
- In der Adresszeile des Web-Browsers geben Sie die Adresse des Geräts vollständig ein (siehe Tabelle 13-4).

Sie gelangen zur Administrator-Webseite des Geräts.

Wenn Sie nicht zur Administrator-Webseite des Geräts gelangen

Falls Sie die konfigurierte Adresse vergessen haben

Falls die Adresse des Geräts im Router- PPPoE- oder PPTP-Modus auf einen anderen Wert gesetzt ist, und Sie die aktuelle Adresse nicht kennen, dann müssen Sie beim Gerät die **Recovery**-Prozedur ausführen, so dass die oben angegebenen Werkseinstellungen der IP-Adresse wieder in Kraft treten (siehe „Recovery-Prozedur ausführen“ auf Seite 267).

Falls die Administrator-Webseite nicht angezeigt wird

Wenn auch nach wiederholtem Versuch der Web-Browser meldet, dass die Seite nicht angezeigt werden kann, versuchen Sie Folgendes:

- Deaktivieren Sie gegebenenfalls bestehende Firewalls.
- Achten Sie darauf, dass der Browser keinen Proxy-Server verwendet.

  Im **Internet Explorer** (Version 8) nehmen Sie diese Einstellung vor: Menü „Extras, Internetoptionen...“, Registerkarte „Verbindungen“.

  Unter „LAN-Einstellungen“ auf die Schaltfläche „Einstellungen“ klicken.

  Im Dialogfeld „Einstellungen für lokales Netzwerk (LAN)“ dafür sorgen, dass unter Proxy-Server der Eintrag „Proxyserver für LAN verwenden nicht“ aktiviert ist.
- Falls andere LAN-Verbindungen auf dem Rechner aktiv sind, deaktivieren Sie diese für die Zeit der Konfiguration.

  Dazu unter Menü „Start, Einstellungen, Systemsteuerung, Netzwerkverbindungen“ bzw. „Netzwerk- und DFÜ-Verbindungen“ auf das betreffende Symbol mit der rechten Maustaste klicken und im Kontextmenü „Deaktivieren“ wählen.

Bei erfolgreichem Verbindungsaufbau

Nach erfolgreicher Verbindungsaufnahme erscheint evtl. ein Sicherheitshinweis.

Erläuterung:

Da das Gerät nur über verschlüsselte Zugänge administrierbar ist, wird es mit einem selbstunterzeichneten Zertifikat ausgeliefert.

- Quittieren Sie den entsprechenden Sicherheitshinweis mit „Ja“.

Das Login-Fenster wird angezeigt.

Bild 13-4 Login

- Geben Sie den voreingestellten Benutzernamen und das voreingestellte Passwort ein, um sich einzuloggen (Groß- und Kleinschreibung beachten):

Benutzername:	admin
Passwort:	mGuard

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren.Informationen dazu finden Sie im Referenzhandbuch zur Software.

Wir empfehlen, aus Sicherheitsgründen bei der ersten Konfiguration das Root- und das Administrator-Passwort zu ändern.

13.7 Fernkonfiguration

Voraussetzung

Das Gerät muss so konfiguriert sein, dass er eine Fernkonfiguration zulässt.

Standardmäßig ist die Möglichkeit zur Fernkonfiguration ausgeschaltet.

Schalten Sie die Möglichkeit zur Fernkonfiguration in der Web-Oberfläche unter „Verwaltung >> Web-Einstellungen“ ein.

Vorgehensweise

Um von einem entfernten Rechner aus das Gerät über seine Web-Oberfläche zu konfigurieren, stellen Sie von dort die Verbindung zum Gerät her.

Gehen Sie wie folgt vor:

- Starten Sie dazu auf dem entfernten Rechner den Web-Browser.
- Als Adresse geben Sie die IP-Adresse an unter der das Gerät von extern über das Internet bzw. WAN erreichbar ist und gegebenenfalls zusätzlich die Port-Nummer.

Beispiel

Wenn das Gerät beispielsweise über die IP-Adresse https://123.45.67.89/ über das Internet zu erreichen ist und für den Fernzugang die Port-Nummer 443 festgelegt ist, dann muss bei der entfernten Gegenstelle im Web-Browser folgende Adresse angegeben werden: https://123.45.67.89/

Bei einer anderen Port-Nummer müssen Sie die Port-Nummer hinter der IP-Adresse angeben, z. B.: https://123.45.67.89:442/

Konfiguration

Anschließend können Sie das Gerät über die Web-Oberfläche konfigurieren. Informationen dazu finden Sie im Referenzhandbuch zur Software.

13.8 Serielle Schnittstelle

Über die serielle Schnittstelle (RS-232) kann eine Benutzer auf die Kommandozeile des Geräts zugreifen. Folgende Parameter müssen gerätespezifisch konfiguriert werden:

– Baudrate: 57600
– Data bits / parity bit / stop bit: 8-N-1
– Hardware-Handshake RTS/CTS: Aus (Voreinstellung)

13.9 Neustart, Recovery-Prozedur und Flashen der Firmware

Die Reset-Taste wird benutzt, um das Gerät in einen der folgenden Zustände zu bringen:

– Neustart durchführen
– Recovery-Prozedur ausführen
– Flashen der Firmware / Rescue-Prozedur

Bild 13-5 Reset-Taste

13.9.1 Neustart durchführen

Ziel

Das Gerät wird mit den konfigurierten Einstellungen neu gestartet.

Aktion

- Drücken Sie die Reset-Taste für ca. 1,5 Sekunden bis die LED ERR leuchtet (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

13.9.2 Recovery-Prozedur ausführen

Ziel (bis 8.3.x)

Bis mGuard-Firmwareversion 8.3.x

Die Netzwerkkonfiguration (aber nicht die restliche Konfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Verwenden Sie die Recovery-Prozedur, wenn Sie die IP-Adresse vergessen haben, unter der das Gerät erreichbar ist.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 13-5 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Das Gerät wird in den Stealth-Modus mit der Werkseinstellung „mehrere Clients“ zurückgesetzt.

– Es wird auch das CIFS-Integrity-Monitoring abgeschaltet, weil es nur mit aktivierter Management-IP funktioniert.
– Weiterhin wird für die Ethernet-Anschlüsse die automatische MAU-Konfiguration aktiviert. Der HTTPS-Zugriff wird über den lokalen Ethernet-Anschluss (LAN) freigegeben.
– Die konfigurierten Einstellungen für VPN-Verbindungen und Firewall bleiben erhalten, ebenso die Passwörter.

Mögliche Gründe zum Ausführen der Recovery-Prozedur:

– Das Gerät befindet sich im Router- oder PPPoE-Modus.
– Die IP-Adresse des Geräts ist abweichend von der Standardeinstellung konfiguriert worden.
– Sie kennen die aktuelle IP-Adresse des Gerätes nicht.

Aktuelle Informationen zur Recovery- und Flash-Prozedur finden Sie in der Application Note, die für Ihre mGuard Firmware-Version relevant ist. Application Notes finden Sie unter folgender Internet-Adresse: phoenixcontact.net/products.

Ziel (ab 8.4.0)

Ab mGuard-Firmwareversion 8.4.0

Die gesamte Konfiguration (und nicht nur die Netzwerkkonfiguration) soll in den Auslieferungszustand zurückgesetzt werden, weil auf das Gerät nicht mehr zugegriffen werden kann.

Die aktuelle Konfiguration wird automatisch auf dem Gerät gespeichert und kann nach erfolgter Recovery-Prozedur wieder hergestellt werden.

Bei der Recovery-Prozedur wird die folgende Netzwerkeinstellung wiederhergestellt:

Tabelle 13-6 Wiederhergestellte Netzwerkeinstellung

Netzwerk-Modus	Management-IP #1	Management-IP #2
Stealth	https://1.1.1.1/	https://192.168.1.1/

Ablauf der Recovery-Prozedur ab mGuard-Firmwareversion 8.4.0

Vor der Durchführung der Recovery-Prozedur wird die aktuelle Konfiguration des Geräts in einem neu erstellten Konfigurationsprofil gespeichert („Recovery-DATUM“). Das Gerät startet nach der Recovery-Prozedur mit den werkseitigen Voreinstellungen.

Das Konfigurationsprofil mit der Bezeichnung „Recovery-DATUM“) erscheint anschließend in der Liste der Konfigurationsprofile und kann bearbeitet und mit oder ohne Änderungen wiederhergestellt werden.

Aktion

- Die Reset-Taste langsam 6-mal drücken.
  Nach ca. 2 Sekunden leuchtet die LED STAT grün.
- Wenn die LED STAT erloschen ist, drücken Sie die Reset-Taste erneut langsam 6-mal.
  Bei Erfolg leuchtet die LED STAT grün
  Bei Misserfolg leuchtet die LED ERR rot

Bei Erfolg vollzieht das Gerät nach 2 Sekunden einen Neustart und schaltet sich dabei auf den Stealth-Modus. Dann ist das Gerät wieder unter den entsprechenden Adressen zu erreichen.

Ab mGuard-Firmwareversion 8.4.0

- Melden Sie sich nach Abschluss der Recovery-Prozedur auf der Weboberfläche des Geräts an.
- Öffnen Sie das Menü **Verwaltung >> Konfigurationsprofile**.
- Wählen Sie das bei der Recovery-Prozedur erstellte Konfigurationsprofil mit dem Namen „Recovery-DATUM“ (z. B. „Recovery-2016.12.01-18:02:50“).
- Klicken Sie auf das Icon „Profil bearbeiten“, um das Konfigurationsprofil zu analysieren und anschließend mit oder ohne Änderungen wiederherzustellen.
- Klicken Sie auf das Icon „Übernehmen“, um die Änderungen zu übernehmen.

13.9.3 Flashen der Firmware / Rescue-Prozedur

Für weitere Informationen siehe auch Anwenderhinweis Update und Flash FL/TC MGUARD auf Version 8.7.x, erhältlich unter phoenixcontact.net/products.

Ziel

Die gesamte mGuard-Firmware soll neu in das Gerät geladen werden.

- **Alle konfigurierten Einstellungen werden gelöscht.** Das Gerät wird in den Auslieferungszustand versetzt.
- Ab mGuard-Firmwareversion 5.0.0 bleiben die im Gerät installierten Lizenzen nach Flashen der Firmware erhalten. Sie müssen also nicht erneut eingespielt werden.

Mögliche Gründe

Das Administrator- und Root-Passwort sind verloren gegangen.

Voraussetzungen

Voraussetzungen für das Flashen

ACHTUNG: Beim Flashen wird die Firmware immer zuerst von einer SD-Karte geladen. Nur wenn keine SD-Karte gefunden wird, wird die Firmware von einem TFTP-Server geladen.

Voraussetzung für das Laden der Firmware von einer SD-Karte ist:

- alle notwendigen Firmware-Dateien müssen in einem gemeinsamen Verzeichnis auf der ersten Partition der SD-Karte vorhanden sein,
- diese Partition nutzt ein VFAT-Dateisystem (Standard bei SD-Karten).

Zum Flashen der Firmware von einem TFTP-Server muss ein TFTP-Server auf dem lokal angeschlossenen Rechner installiert sein (siehe „DHCP- und TFTP-Server installieren“ auf Seite 276).

ACHTUNG: Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

- Sie haben die Firmware des Geräts vom Support Ihres Händlers oder von der Web-Site phoenixcontact.net/products bezogen und auf eine kompatible SD-Karte gespeichert.
- Diese SD-Karte ist im Gerät eingesetzt.
- Auf der Download-Seite von phoenixcontact.net/products stehen die entsprechenden Firmware-Dateien zum Herunterladen bereit. Auf der SD-Karte müssen die Dateien unter diesen Pfadnamen oder in diesen Ordnern liegen:

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

Aktion

Gehen Sie zum Flashen der Firmware bzw. zur Durchführung der Rescue-Prozedur wie folgt vor:

ACHTUNG: Sie dürfen während der gesamten Flash-Prozedur auf keinen Fall die Stromversorgung des Geräts unterbrechen! Das Gerät könnte ansonsten beschädigt werden und nur noch durch den Hersteller reaktiviert werden.

- Halten Sie die Reset-Taste gedrückt, bis die LEDs STAT, MOD und SIG grün leuchten. Dann ist das Gerät im Rescue-Status.
- **Lassen Sie spätestens 1 Sekunde nach Eintritt des Rescue-Status die Reset-Taste los.**

  Falls Sie die Reset-Taste nicht loslassen, wird das Gerät neu gestartet.

  Das Gerät startet nun das Rescue-System: Er sucht zunächst nach einer eingelegten SD-Karte und dort nach der entsprechenden Firmware.Wird keine SD-Karte gefunden, sucht das Gerät über die LAN-Schnittstelle nach einem DHCP-Server, um von diesem eine IP-Adresse zu beziehen.

  Die LED STAT blinkt.

  Vom TFTP-Server oder von der SD-Karte wird die Datei install.p7s geladen. Diese enthält die elektronisch unterschriebene Kontrollprozedur für den Installationsvorgang. Nur unterschriebene Dateien werden ausgeführt.

  Die Kontrollprozedur löscht den aktuellen Inhalt des Flashspeichers und bereitet die Neuinstallation der Firmware vor.

  Die LEDs STAT, MOD und SIG bilden ein Lauflicht

  Vom TFTP-Server oder von der SD-Karte wird die Firmware jffs2.img.p7s heruntergeladen und in den Flashspeicher geschrieben. Diese Datei enthält das eigentliche mGuard-Betriebssystem und ist elektronisch signiert. Nur von Phoenix Contact signierte Dateien werden akzeptiert.

  Dieser Vorgang dauert ca. 3 bis 5 Minuten. Die LED STAT leuchtet kontinuierlich.

  Die neue Firmware wird entpackt und konfiguriert. Das dauert ca. 1 – 3 Minuten.

Sobald die Prozedur beendet ist, blinken die LEDs STAT, MOD und SIG gleichzeitig grün.

- Starten Sie das Gerät neu. Drücken Sie dazu kurz die Reset-Taste.

  (Alternativ können Sie die Stromversorgung unterbrechen und wieder anschließen.)

Das Gerät befindet sich im Auslieferungszustand. Konfigurieren Sie ihn neu (siehe „Lokale Konfigurationsverbindung herstellen“ auf Seite 263).

13.10 Technische Daten

Hardware-Eigenschaften	FL MGUARD DELTA TX/TX
Plattform	Freescale Netzwerkprozessor mit 330 MHz Taktung
Netzwerk-Schnittstellen	1 LAN-Port | 1 WAN-Port Ethernet IEEE 802.3 10/100 Base TX | RJ 45 | Full Duplex | Auto-MDIX
Sonstige Schnittstellen	seriell RS-232, D-SUB 9-Stecker
Speicher	128 MB RAM | 128 MB Flash SD-Karte, wechselbarer Konfi gurationsspeicher
Redundanz-Optionen	optional: VPN | Router
Stromversorgung	externes Netzteil 12V / 0,85A DC | 100–240V / 0,4A AC
Leistungsaufnahme	typisch 2,13 Watt
Luftfeuchtigkeitsbereich	5 % ... 95 % in Betrieb, nicht kondensierend
Schutzart	IP20
Temperaturbereich	0 °C ... +40 °C (Betrieb) 0 °C ... +60 °C (Lagerung)
Maße (H x B x T)	45 x 130 x 114 mm
Gewicht	725 g
Gewicht (inkl. Verpackung)	1025 g

Firmware und Leistungswerte	FL MGUARD DELTA TX/TX
Firmware-Kompatibilität	mGuard v7.4.0 oder höher; Phoenix Contact empfiehlt die Verwendung der jeweils aktuellen Firmware-Version und Patch Releases Funktionsumfang siehe entsprechendes Firmware-Datenblatt
Datendurchsatz (Firewall)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 120 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 50 MBit/s
Virtual Private Network (VPN)	IPsec (IETF-Standard), VPN-Modelle bis 10 Tunnel, optional bis zu 250 VPN-Tunnel
Hardware-basierte Verschlüsselung	DES | 3DES | AES-128/192/256
Datendurchsatz verschlüsselt (IPsec VPN)	Router-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 30 MBit/s Stealth-Modus, Default Firewall-Regeln, bidirektionaler Durchsatz: max. 20 MBit/s
Management Support	Web GUI (HTTPS) | Command Line Interface (SSH) | SNMP v1/2/3 | zentrale Device Management Software
Diagnose	LEDs (Power, State, Error, Fault, Info) | Log-File | Remote-Syslog

Sonstiges	FL MGUARD DELTA TX/TX
Konformität	CE | FCC
Besonderheiten	Echtzeituhr | Trusted Platform Module (TPM) | Temperatursensor | mGuard Remote Services Portal ready

14 IP-Adressen vergeben und DHCP/TFTP-Server einrichten

14.1 Vergabe der IP-Adresse mit IPAssign.exe

Schritt 1: Programm herunterladen und ausführen

- Wählen Sie im Internet den Link phoenixcontact.net/products.
- Geben Sie in der Suchmaske den Suchbegirff „ipassign“ ein.
- Wählen Sie das gewünschte oder ein beliebiges anderes Produkt.

Unter „Download“ und „Software“ finden Sie das gewünschte Programm.

- Doppelklicken Sie auf die Datei „IPAssign.exe“.
- Wählen Sie im sich öffnenden Fenster die Schaltfläche „Ausführen“.

Schritt 2: „IP Assignment Wizard“

Das Programm wird geöffnet und der Startbildschirm des Adressierungs-Tools erscheint.

Das Programm ist in großen Teilen in Englisch gehalten. Die Schaltflächen des Programms passen sich an die landesspezifischen Einstellungen an.

Auf dem Startbildschirm wird die IP-Adresse des PCs angezeigt. Dies hilft in den weiteren Schritten bei der Adressierung des mGuards.

- Wählen Sie auf die Schaltfläche „Weiter“.

Schritt 3: „IP Address Request Listener“

Im sich öffnenden Fenster werden alle Geräte, die einen BootP-Request senden, gelistet und warten auf eine neue IP-Adresse.

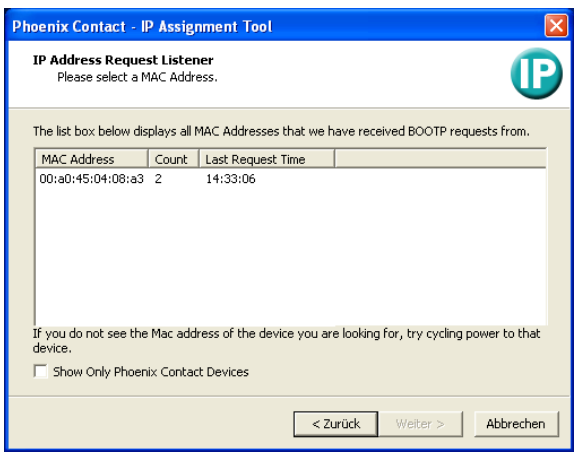


Bild 14-1 Fenster „IP Address Request Listener“

Im gezeigten Beispiel hat der mGuard die MAC-ID 00.A0.45.04.08.A3.

- Wählen Sie das Gerät, dem Sie eine IP-Adresse vergeben wollen, aus.
- Wählen Sie die Schaltfäche „Weiter“.

Schritt 4: „SET IP Address“

Im sich öffnenden Fenster werden folgende Informationen angegeben:

– IP-Adresse des PCs
– MAC-Adresse des ausgewählten Geräts
– IP-Parameter des ausgewählten Geräts
(IP-Adresse, Subnetzmaske und Gateway-Adresse)
– Eventuelle fehlerhafte Einstellungen

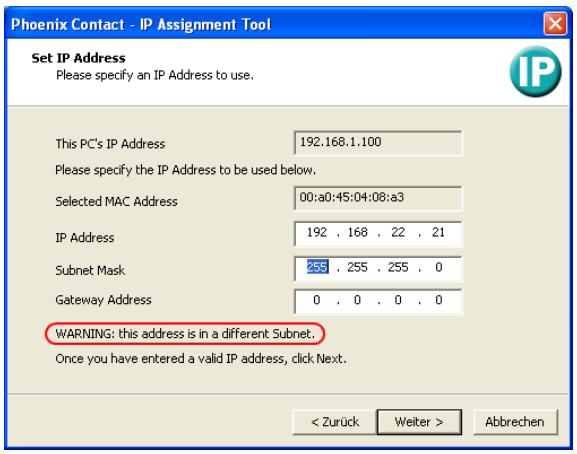


Bild 14-2 Fenster „Set IP Address“ mit fehlerhaften Einstellungen

- Passen Sie die IP-Parameter an Ihre Gegebenheiten an.

Wenn keine Unstimmigkeiten mehr erkannt werden, erscheint die Information, dass eine gültige IP-Adresse eingestellt wurde.

- Wählen Sie die Schaltfäche „Weiter“.

Schritt 5: „Assign IP Address“

Das Programm versucht, die eingestellte IP-Parameter an den mGuard zu übertragen.

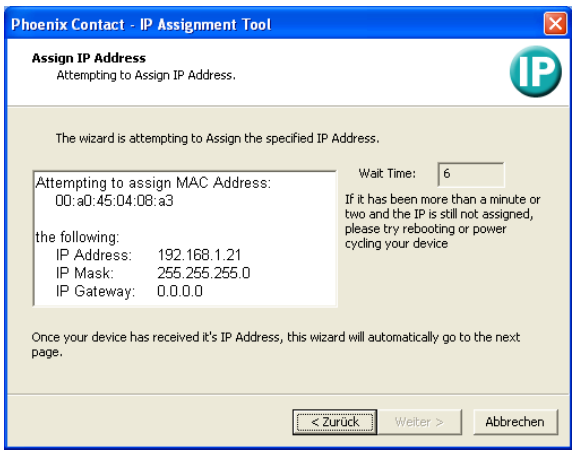


Bild 14-3 Fenster „Assign IP Address“

Nach erfolgreicher Übertragung öffnet sich das nächste Fenster.

Schritt 6: Abschluss der IP-Adressvergabe

Das folgenden Fenster informiert Sie über den erfolgreichen Abschluss der Adressvergabe. Sie erhalten eine Übersicht darüber, welche IP-Parameter an das Gerät mit der angezeigten MAC-Adresse übertragen wurden.

Wenn Sie IP-Parameter für weitere Geräte vergeben wollen:

- Wählen Sie die Schaltfäche „Zurück“.

Wenn Sie die IP-Adressvergabe beenden wollen:

- Wählen Sie die Schaltfäche „Fertig stellen“.

Die hier eingestellten IP-Parameter können Sie bei Bedarf in der mGuard Web-Oberfläche unter „Netzwerk >> Interfaces“ ändern.

14.2 DHCP- und TFTP-Server installieren

Falls Sie einen zweiten DHCP-Server in einem Netzwerk installieren, könnte dadurch die Konfiguration des gesamten Netzwerks beeinflusst werden.

Software von Drittanbietern

Phoenix Contact übernimmt keine Garantie oder Haftung bei der Verwendung von Produkten von Drittanbietern. Verweise auf Drittanbieter-Software stellen keine Empfehlung dar, sondern sind Beispiele für grundsätzlich verwendbare Programme.

Unter Windows

Falls Sie das Drittanbieter-Programm „TFTPD32.exe“ verwenden wollen, beschaffen Sie sich das Programm aus einer vertrauenswürdigen Quelle und gehen Sie wie folgt vor:

- Wenn der Windows-Rechner an ein Netzwerk angeschlossen ist, trennen Sie ihn von diesem.
- Kopieren Sie die Firmware in einen beliebigen leeren Ordner des Windows-Rechners.
- Starten Sie das Programm TFTPD32.EXE

Die festzulegende Host-IP lautet: **192.168.10.1.** Das muss auch die Adresse für die Netzwerkkarte sein.

- Klicken Sie die Schaltfläche **Browse**, um auf den Ordner zu wechseln, wo die mGuard-Image-Dateien gespeichert sind: **install.p7s, jffs2.img.p7s**
- Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** oder der Seriennummer des zugehörigen Geräts **<Seriennummer>.lic** (z. B. 2138413892.lic) ebenfalls dort abgelegt werden.

  Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, die wirklich zum Gerät gehört (in der Web-Oberfläche unter „Verwaltung >> Update“).

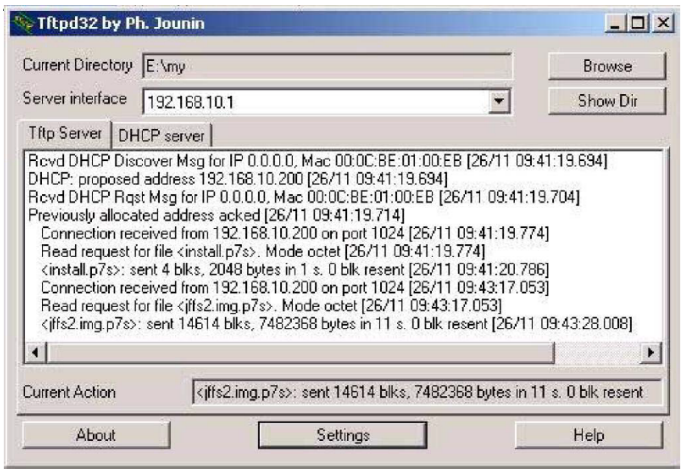
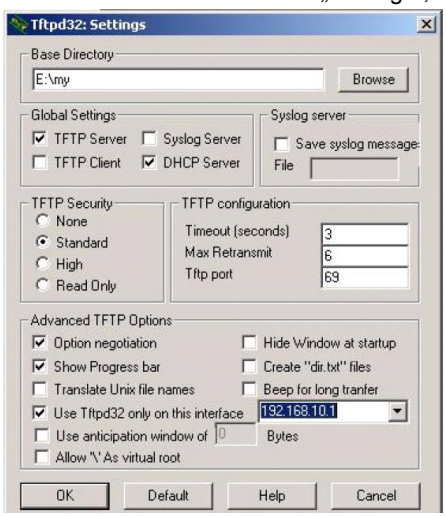


Bild 14-4 Host-IP eingeben

- Wechseln Sie auf die Registerkarte „TFTP-Server“ bzw. „DHCP-Server“ und klicken Sie dann die Schaltfläche „Settings“, um die Parameter wie folgt zu setzen:



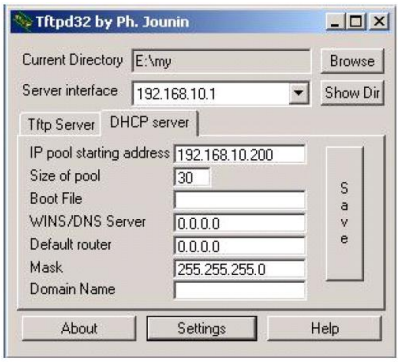


Bild 14-5 Settings

Unter Linux

Alle aktuellen Linux-Distributionen enthalten DHCP- und TFTP-Server.

- Installieren Sie die entsprechenden Pakete nach der Anleitung der jeweiligen Distribution.
- Konfigurieren Sie den DHCP-Server, indem Sie in der Datei **/etc/dhcpd.conf** folgende Einstellungen vornehmen:

  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;}

Diese Beispiel-Konfiguration stellt 20 IP-Adressen (.100 bis .119) bereit. Es wird angenommen, dass der DHCP-Server die Adresse 192.168.134.1 hat (Einstellungen für ISC DHCP 2.0).

Der benötigte TFTP-Server wird in folgender Datei konfiguriert: **/etc/inetd.conf**

- Fügen Sie in diese Datei die entsprechende Zeile ein oder setzen Sie die notwendigen Parameter für den TFTP-Service. (Verzeichnis für Daten ist: **/tftpboot)**

  tftp dgram udp wait root /usr/sbin/in.tftpd -s /tftpboot/

Im Verzeichnis **/tftpboot** müssen die mGuard-Imagedateien gespeichert sein: **install.p7s, jffs2.img.p7s**

- Falls durch das Flashen ein Major-Release-Upgrade der Firmware vorgenommen wird, muss die für das Upgrade erworbene Lizenz-Datei unter dem Namen **licence.lic** oder der Seriennummer des zugehörigen Geräts **<Seriennummer>.lic** (z. B. 2138413892.lic) ebenfalls dort abgelegt werden.

  Stellen Sie sicher, dass es sich um die Lizenzdatei handelt, welche wirklich zum Gerät gehört (in der Web-Oberfläche unter „Verwaltung >> Update“).
- Starten Sie dann den inetd-Prozess neu, um die Konfigurationsänderungen zu übernehmen.

- Wenn Sie einen anderen Mechanismus verwenden, z. B. xinetd, dann informieren Sie sich in der entsprechenden Dokumentation.