Rittal – The System.

Faster – better – everywhere.

**PDU**
metered
metered plus
switched
managed

7979.XXX (Dabei kann X eine beliebige Zahl zwischen 0 und 9 sein)

Regulatory model code:
DK01, DK02, DK03, DK04

# System Hardening Guide

DE

## Inhaltsverzeichnis

DE

## 1 Einleitung

Produkte, Netzwerke und Systeme müssen vor unberechtigten Zugriffen geschützt werden, um die
Verfügbarkeit, die Vertraulichkeit und die Integrität von Daten zu gewährleisten.
Dies muss durch organisatorische und technische Maßnahmen umgesetzt werden.
Für erhöhte Sicherheitsanforderungen empfiehlt Rittal die folgenden Maßnahmen zu beachten.
Dabei gibt es nicht nur Hinweise zur sicheren Nutzung, sondern auch zu konkreten Einstellungen am Gerät, die die Sicherheit erhöhen.
Es gilt in der Praxis immer abzuwägen, inwiefern eine der beschriebenen Änderungen angewandt werden
sollte oder nicht.
Die verfügbaren Einstellungen können sich je nach eingesetztem Gerät unterscheiden.
Darüber hinaus finden Sie weiterführende Informationen auf den Webseiten des Bundesamts für Sicherheit in
der Informationstechnik:

- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html
- https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Angriffszielen/Industrielle-Steuerungs-und-Automatisierungssysteme/Allgemeine-Empfehlungen/allgemeine-empfehlungen_node.html

## 2 Allgemeine Hinweise

Bitte beachten Sie die allgemeinen IT-Sicherheitshinweise im Handbuch Ihres Gerätes.

- Betreiben Sie das Gerät nicht direkt im Internet, sondern nur in internen Netzwerken, die durch Firewalls nach außen abgesichert sind.
- Beschränken Sie die Zugangsberechtigungen zu den Geräten auf die Personen, die eine Berechtigung unbedingt benötigen.
- Beschränken Sie den physischen Zugang zu den Geräten durch geeignete Maßnahmen.

DE

# 3 Kommunikationskanäle

Grunsätzlich gilt das Sie alle nicht genutzten Kommunikationskanäle am Gerät deaktivieren sollten.
Darüberhinaus stehen für viele Protokolle Alternativen mit höherer Sicherheit zu Verfügung. Hier wird empfohlen die unsichere Variante zu deaktiveren. Bei einigen Protokollen kann die Sicherheit noch durch weitere Einstellungen erhöht werden.

## 3.1 HTTP (Webzugriff)

Der Zugriff auf die Webseite des Gerätes darf nur über HTTPS erfolgen. Dabei wird empfohlen das "Security Level" auf "Modern" zu setzen um die Nutzung von TLS 1.3 zu forcieren.

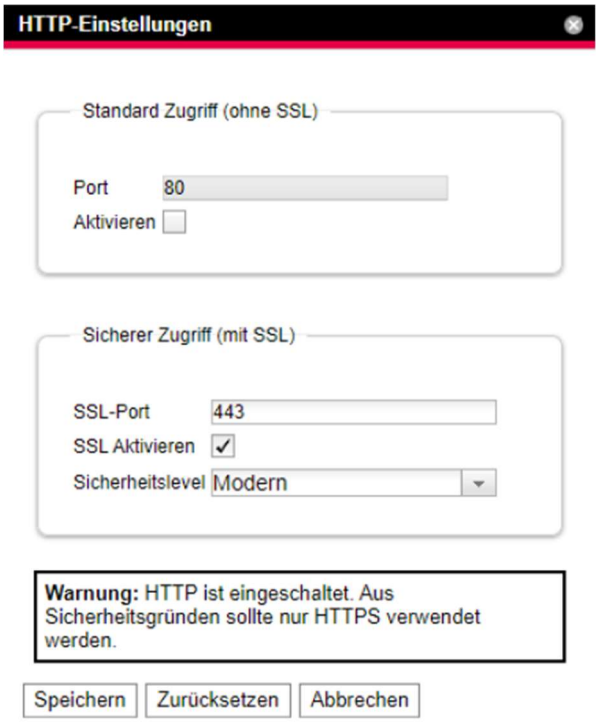


Abbildung 1: HTTP Einstellungen

## 3.2 Dateitransfer

Der Zugriff auf das Gerät über FTP/SFTP ist generell zu deaktivieren. Der SFTP Zugang sollte nur für die Dauer einer Aufgabe (z.B. Software-Update oder Datensicherung, siehe Handbuch) aktiviert werden.

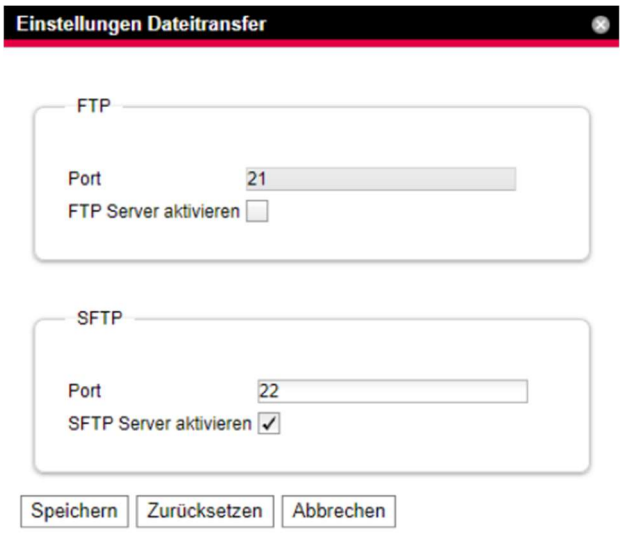


Abbildung 2: Einstellungen Dateitransfer

## 3.3 Konsole

Es wird empfohlen den Konsolen Zugang über Telnet komplett zu deaktivieren, da die Übertragung unverschlüsselt erfolgt.

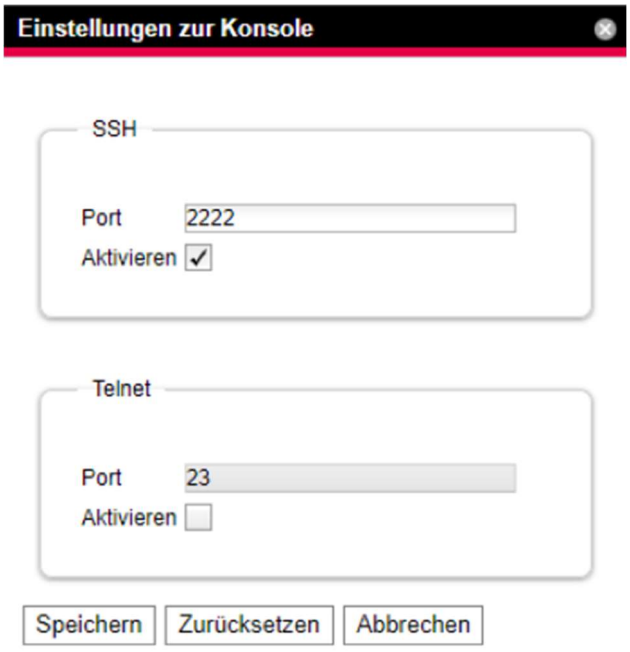


Abbildung 3: Einstellungen zur Konsole

## 3.4 SMTP

Bei der Nutzung von SMTP ist zu beachten, dass der genutzte Mailserver Authentifizierung und Verschlüsselung unterstützt.

DE

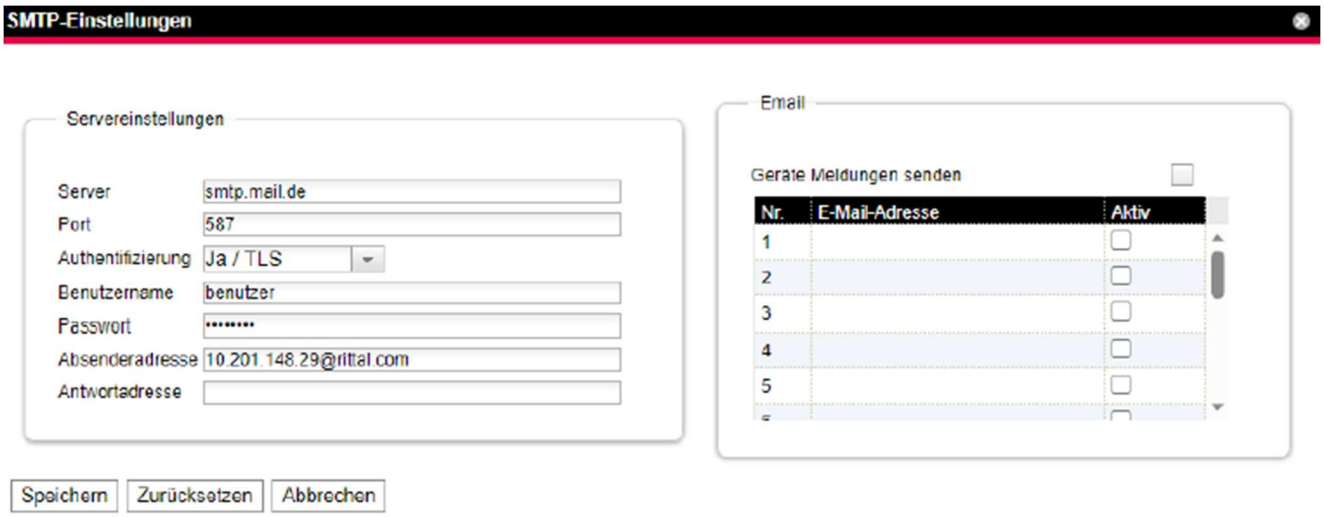


Abbildung 4: SMTP Einstellungen

## 3.5 SNMP

Bei der Verwendung von SNMP ist darauf zu achten, nur Version 3 einzusetzen, da Version 1 und 2 keine Möglichkeiten der Authentifizierung und Verschlüsselung bieten.

In den Einstellungen wird empfohlen die "Authentifizierungsmethode auf "SHA" und die "Privatsphäre" auf "AES" zu stellen. Außerdem sind die Standard Communities „public“ bei SNMP zu überschreiben.

Aktuell wird auf dem Gerät bei SNMP nur SHA1 unterstützt, sollte dies in der Anwendung/Umgebung nicht den Anforderungen entsprechen, darf SNMP nicht genutzt werden.

Bei der Passwortvergabe ist zu beachten, dass dieses den im Kapitel "Sichere Passwörter" vorgestellten Regeln genügt.

Weiterhin wird empholen in der Sektion "Allowed Hosts" alle Hosts einzutragen, welche über SNMP auf das Gerät zugreifen dürfen.

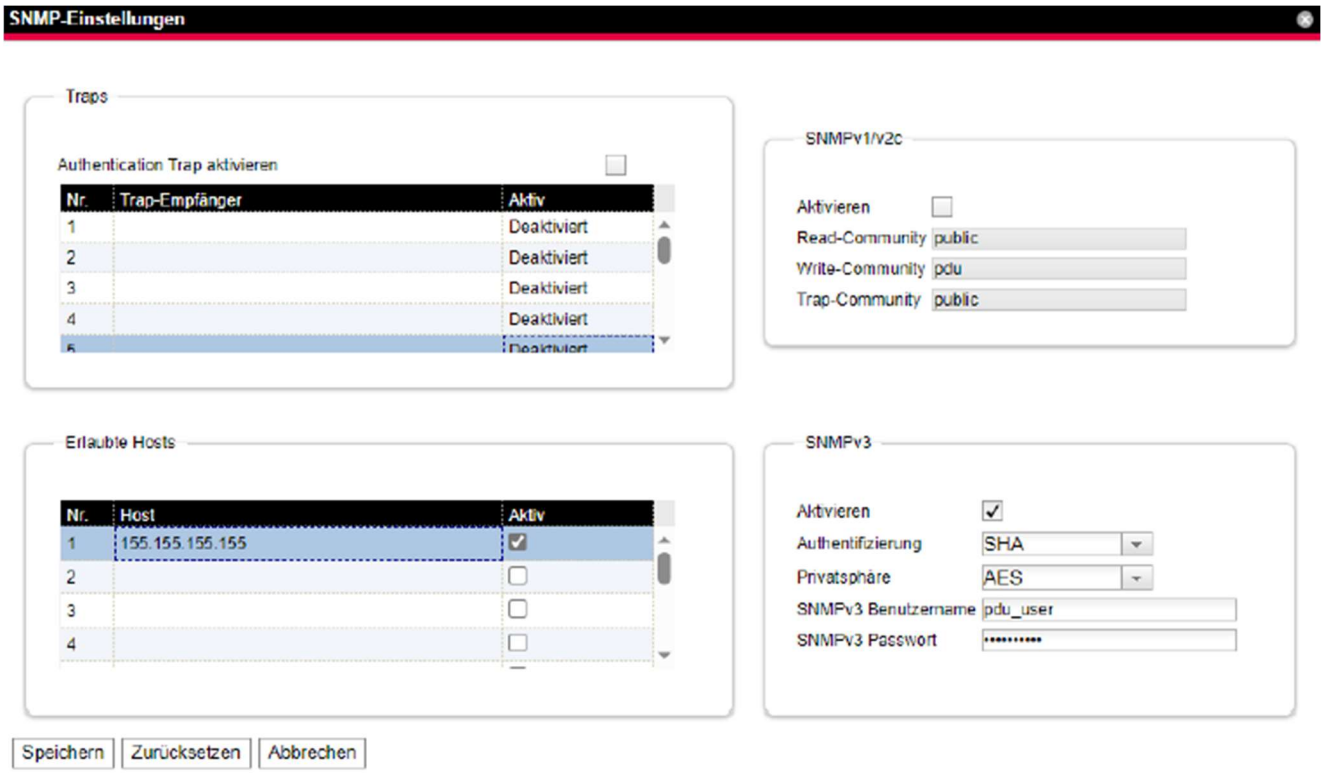


Abbildung 5: SNMP Einstellungen

## 3.6 Modbus/TCP

Das Modbus Protokoll bietet keine Authentifizierungs- und Verschlüsselungs-Funktion und von der Nutzung wird daher abgeraten.

Lässt sich der Einsatz nicht vermeiden, wird empfohlen, die Hosts, welche über Modbus auf das Gerät zugreifen dürfen, in der Sektion "Allowed Hosts" einzutragen. Außerdem wird empfohlen, den Zugriff wenn möglich auf "lesenden Zugriff" zu beschränken.

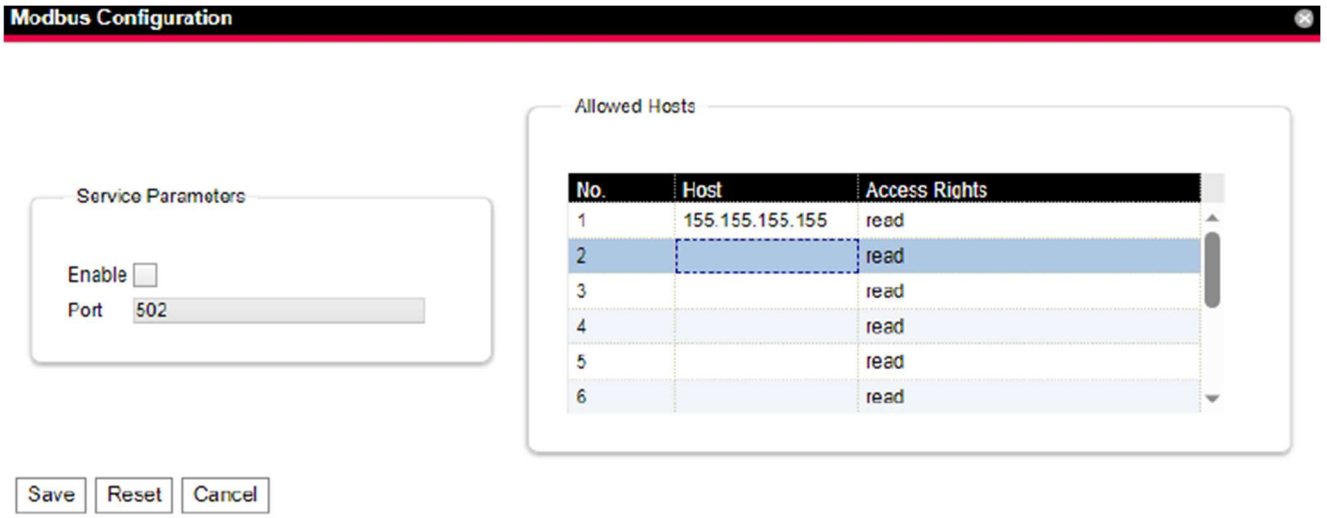


Abbildung 6: Modbus Konfiguration

## 3.7 OPC-UA

Aktuell bieten die Geräte keine Möglichkeit Zugriffe über OPC-UA zu verschlüsseln.

Wenn OPC-UA dennoch benötigt wird, wir empfohlen, die Benutzer Authentifizierung unter dem Dropdown "Security" anschalten und ein sicheres Passwort zu vergeben.

DE

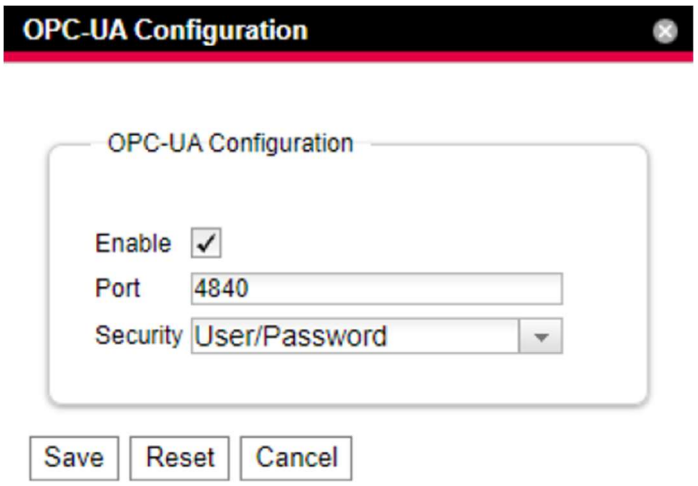


Abbildung 7: OPC-UA Konfiguration

# 4 Dateiaustausch und Updates

## 4.1 Aktuelle Sicherheits-Software

Für die Identifizierung und Eliminierung von Sicherheitsrisiken wie Viren, Trojanern und anderer Schadsoftware, wird empfohlen auf allen PCs eine Sicherheits-Software installiert zu haben und diese aktuell zu halten.

Jegliche Daten, die auf das Gerät gespielt werden, sind vom Anwender zu überprüfen.

## 4.2 Aktuelle Firmware-Version

Stellen Sie sicher, dass auf allen Geräten die aktuelle Rittal – Firmware verwendet wird. Die Firmware wird auf

den jeweiligen Produktseiten im Internet zum Download bereitgestellt.

## 4.3 Schnittstellen

Obwohl das Gerät nur bekannte und signierte Daten vom Gerät akzeptiert und verarbeitet, wird empfohlen, die Schnittstellen (z.B. USB) zu deaktiveren.

Dies erfolgt im Bereich Überwachung und die Einstellung findet sich dann im Gerätebaum unter dem Punkt "Memory". Dort kann das entsprechende "Command" zum Abschalten der USB-Schnittstelle ("Aus") geschrieben werden.

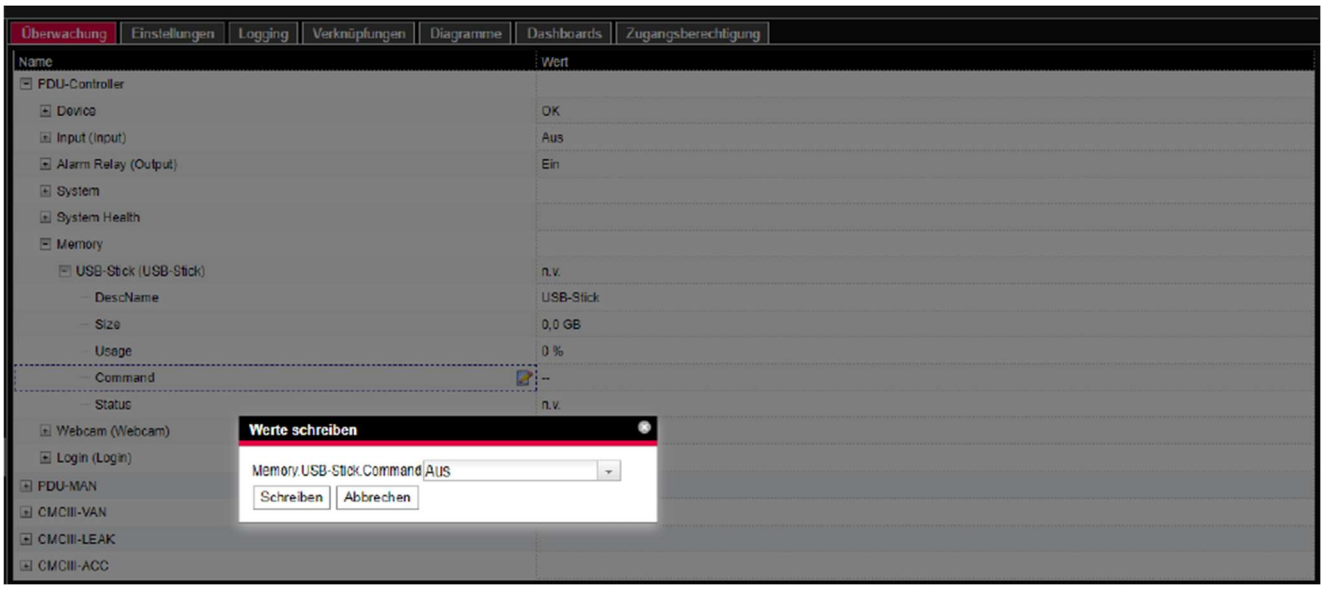


Abbildung 8: USB-Stick Konfiguration

# 5 Zugangsberechtigungen

Nicht genutzte Benutzerkonten sind zu deaktiveren.

Sofern möglich, wird der Einsatz von zentralen Nutzerverwaltungen für das User-Management und die Anmeldeinformationen empfohlen.

## 5.1 Admin Berechtigungen

Beachten Sie, das Nutzer, welche einer Gruppe mit aktiviertem Admin-Flag angehören, über das Web Management Interface Zugriff auf die komplette Gerätekonfiguration haben und alle Einstellungen herunterladen und bearbeiten können.

Die Zahl der Benutzer mit Admin Berechtigungen bzw. Admin Gruppen Zugehörigkeit ist auf notwendige vertrauenswürdige Personen zu beschränken.

## 5.2 Dateitransfer Berechtigung

Nutzer bei denen der Dateitransfer erlaubt ist, können auf alle auf dem Gerät liegenden Daten zugreifen und bei aktiviertem Schreibzugriff auch verändern. Dazu gehören auch Statusinformationen und die Gerätekonfiguration. Dies erfolgt unabhängig der Zugehörigkeit zu einer Gruppe mit aktiviertem Admin Flag.

Der Dateitransfer ist daher nur für Benutzer zu aktiveren, welche Mitglied in einer Gruppe mit Admin Flag sind und sollte, sofern möglich, auf den schreibenden Zugriff verzichtet werden. Nutzer mit Dateitransfer Berechtigung sind als Administratoren anzusehen.

## 5.3 Sichere Passwörter

Verwenden Sie nicht die Standard-Passwörter, sondern nur sichere, lange Passwörter, die Zahlen, große/ kleine Buchstaben, Zeichen und keine Wiederholungen beinhalten.

Erzeugen Sie nach Möglichkeit zufällige Passwörter mit einem Passwort-Manager.

## 5.4 Fernzugriffe

Bei der Nutzung von Fernzugriffen ist ein sicherer Zugriffsweg wie VPN (Virtual Private Network) oder HTTPS zu wählen.

# 6 Reset auf Werkseinstellungen

Um das Gerät zurückzusetzen und alle Daten und Einstellungen zu löschen sind folgende Schritte erforderlich:

- Gerät vom Strom trennen.

# 6 Reset auf Werkseinstellungen

DE

- Die Display Taste unter dem R des Rittal-Aufdrucks gedrückt halten
- Gerät mit Spannung versorgen und Taste gedrückt halten bis die Status LED Rot reagiert.
- Ausführen der Wiederherstellung ist erkennbar am weißen Blitzen der Status LED.

# Rittal – The System.

**Faster – better – everywhere.**

- Enclosures
- Power Distribution
- Climate Control
- IT Infrastructure
- Software & Services

You can find the contact details of all
Rittal companies throughout the world here.

www.rittal.com/contact

RITTAL GmbH & Co. KG
Postfach 1662 · 35726 Herborn · Germany
Phone +49 2772 505-0 · Fax +49 2772 505-2319
E-mail: info@rittal.de · www.rittal.com