Rittal – The System.

Faster – better – everywhere.

# PDU
metered
metered plus
switched
managed

7979.XXX (X can be any number from 0 to 9)

Regulatory model code:
DK01, DK02, DK03, DK04

# System Hardening Guide

ENCLOSURES POWER DISTRIBUTION CLIMATE CONTROL IT INFRASTRUCTURE SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

## Inhaltsverzeichnis

# 1 Introduction

Products, networks and systems must be protected against unauthorized access in order to ensure the availability, confidentiality and integrity of data.

This must be implemented through organizational and technical measures. Rittal recommends the following measures for increased security requirements.

There is not only information on secure use, but also on specific settings on the device that increase security.

In practice, it is always necessary to weigh up the extent to which one of the changes described should be applied or not.

The available settings may vary depending on the device used.

You can also find further information on the website of the Federal Office for Information Security:

- 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 General information

Please follow the general IT security instructions in the manual for your device.

- Do not operate the device directly on the Internet, but only in internal networks that are protected from the outside by firewalls.
- Restrict the access authorizations to the devices to those persons who absolutely require authorization.
- Take suitable measures to restrict physical access to the devices.

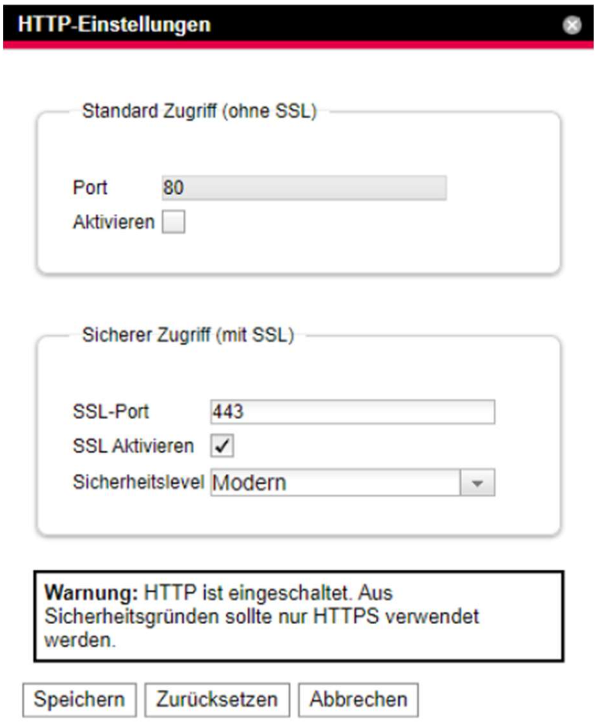
## 3 Channels of communication

As a general rule, you should deactivate all unused communication channels on the device.

In addition, alternatives with higher security are available for many protocols. We recommend deactivating the insecure variant here. For some protocols, security can be increased by making further settings.

### 3.1 HTTP (Web access)

The website of the device may only be accessed via HTTPS. It is recommended to set the "Security Level" to "Modern" to force the use of TLS 1.3.



**HTTP-Einstellungen**

Standard Zugriff (ohne SSL)

Port 80

Aktivieren ☐

Sicherer Zugriff (mit SSL)

SSL-Port 443

SSL Aktivieren ☑

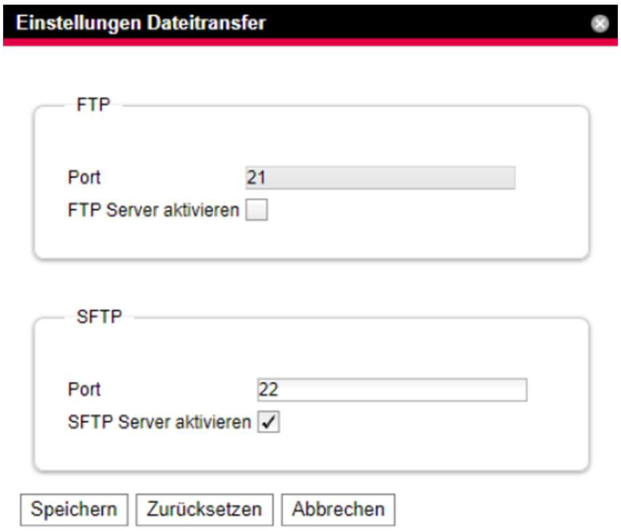
Sicherheitslevel Modern

**Warnung:** HTTP ist eingeschaltet. Aus Sicherheitsgründen sollte nur HTTPS verwendet werden.

Picture 1: HTTP settings

### 3.2 File transfer

Access to the device via FTP/SFTP should generally be deactivated. SFTP access should only be activated for the duration of a task (e.g. software update or data backup, see manual).



**Einstellungen Dateitransfer**

FTP

Port 21

FTP Server aktivieren ☐

SFTP

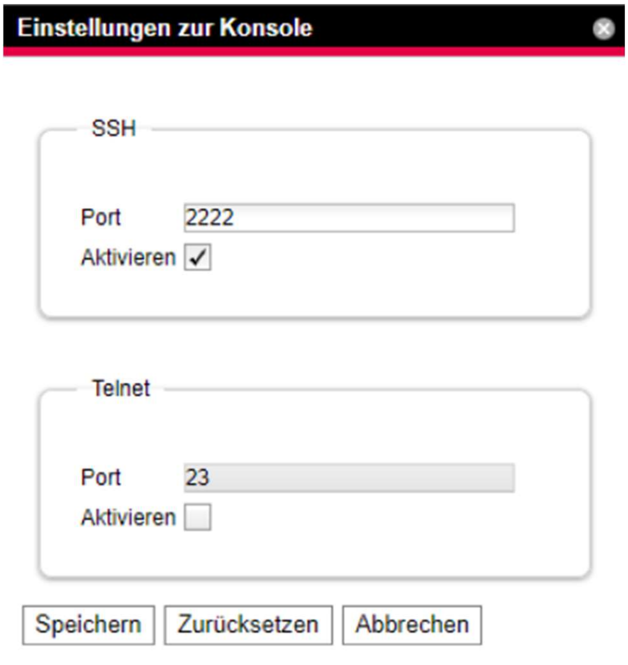
Port 22

SFTP Server aktivieren ☑

Picture 2: File transfer settings

## 3.3 Console

It is recommended to completely deactivate console access via Telnet, as the transmission is unencrypted.



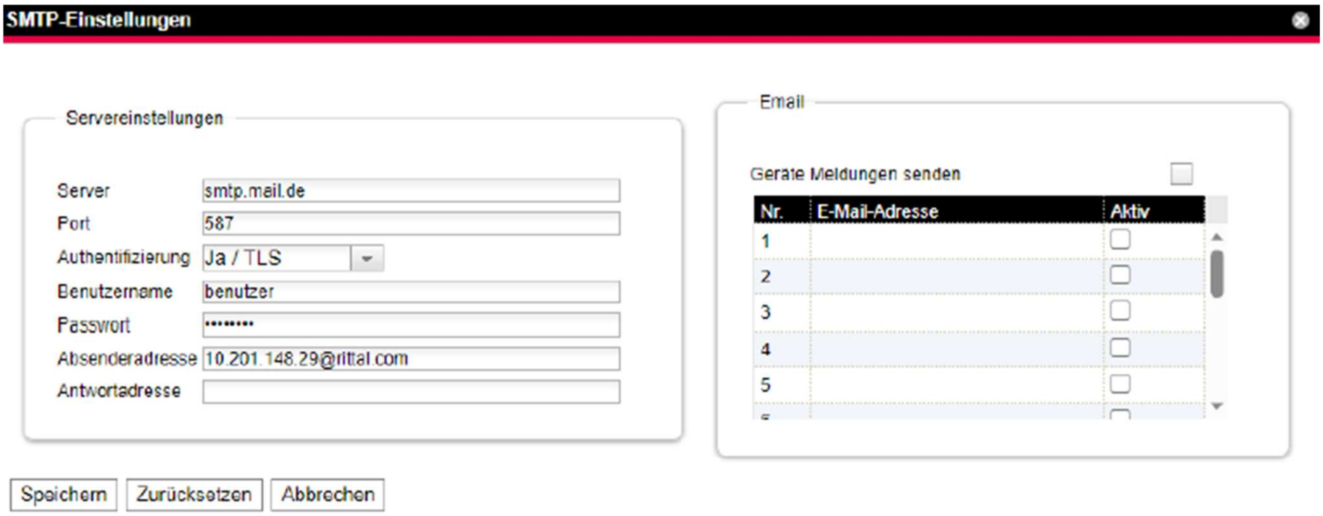
SSH
Port 2222
Aktivieren ☑

Telnet
Port 23
Aktivieren ☐

Picture 3: Console settings

## 3.4 SMTP

When using SMTP, please note that the mail server used must support authentication and encryption.



Servereinstellungen
Server smtp.mail.de
Port 587
Authentifizierung Ja / TLS
Benutzername benutzer
Passwort ••••••••
Absenderadresse 10.201.148.29@rittal.com
Antwortadresse

Email
Gerate Meldungen senden ☐

| Nr. | E-Mail-Adresse | Aktiv |
|---|---|---|
| 1 | | ☐ |
| 2 | | ☐ |
| 3 | | ☐ |
| 4 | | ☐ |
| 5 | | ☐ |

Picture 4: SMTP settings

## 3.5 SNMP

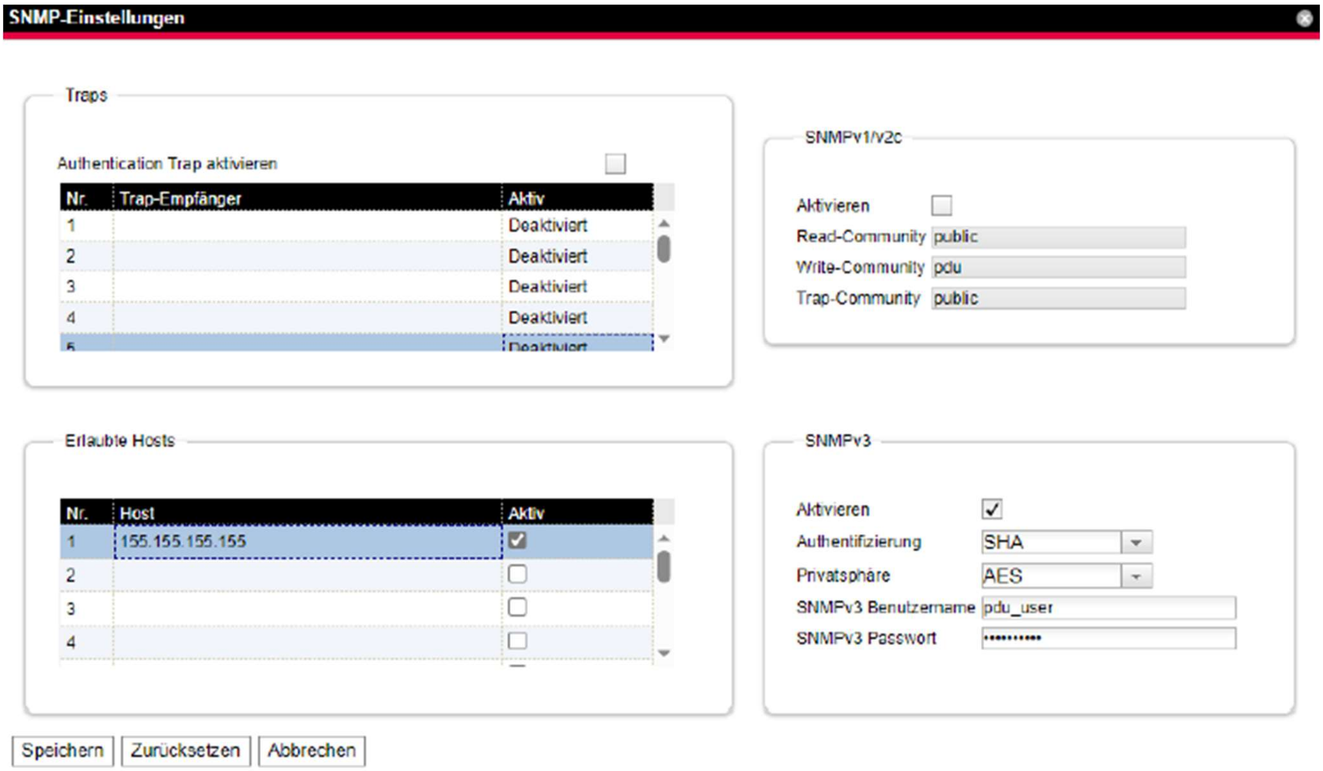
When using SNMP, make sure to only use version 3, as versions 1 and 2 do not offer any authentication and encryption options.

In the settings, it is recommended to set the "Authentication method" to "SHA" and the "Privacy" to "AES". In addition, the default communities "public" for SNMP must be overwritten.

Only SHA1 is currently supported for SNMP on the device; if this does not meet the requirements in the application/environment, SNMP must not be used.

When assigning a password, make sure that it complies with the rules presented in the "Secure passwords" section.

It is also recommended to enter all hosts that are allowed to access the device via SNMP in the "Allowed Hosts" section.



Authentication Trap aktivieren ☐

| Nr. | Trap-Empfänger | Aktiv |
|---|---|---|
| 1 | | Deaktiviert |
| 2 | | Deaktiviert |
| 3 | | Deaktiviert |
| 4 | | Deaktiviert |
| 5 | | Deaktiviert |

Aktivieren ☐
Read-Community public
Write-Community pdu
Trap-Community public

| Nr. | Host | Aktiv |
|---|---|---|
| 1 | 155.155.155.155 | ☑ |
| 2 | | ☐ |
| 3 | | ☐ |
| 4 | | ☐ |

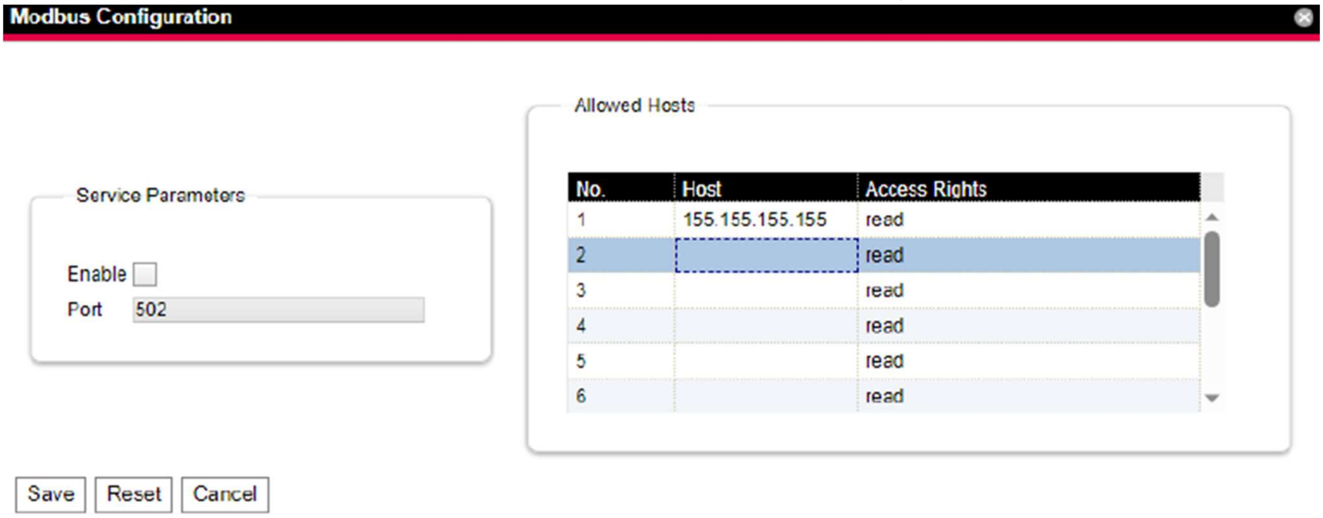
Aktivieren ☑
Authentifizierung SHA
Privatsphäre AES
SNMPv3 Benutzername pdu_user
SNMPv3 Passwort ••••••••••

Picture 5: SNMP settings

## 3.6 Modbus/TCP

The Modbus protocol does not offer an authentication and encryption function and its use is therefore not recommended.

If its use cannot be avoided, it is recommended to enter the hosts that are allowed to access the device via Modbus in the "Allowed Hosts" section. It is also recommended to restrict access to "read access" if possible.



Enable ☐
Port 502

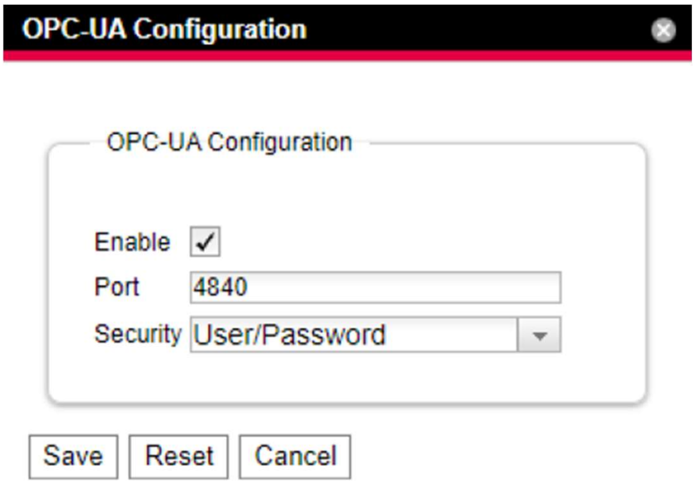
| No. | Host | Access Rights |
|---|---|---|
| 1 | 155.155.155.155 | read |
| 2 | | read |
| 3 | | read |
| 4 | | read |
| 5 | | read |
| 6 | | read |

Picture 6: Modbus configuration

## 3.7 OPC-UA

The devices currently do not offer the option of encrypting access via OPC-UA.

If OPC-UA is still required, we recommend switching on user authentication under the "Security" dropdown and assigning a secure password.



Enable ☑
Port 4840
Security User/Password

Picture 7: OPC-UA configuration

# 4 File exchange and updates

## 4.1 Security software

To identify and eliminate security risks such as viruses, Trojans and other malware, it is recommended to have security software installed on all PCs and to keep it up to date.

Any data that is uploaded to the device must be checked by the user.

## 4.2 Firmware version

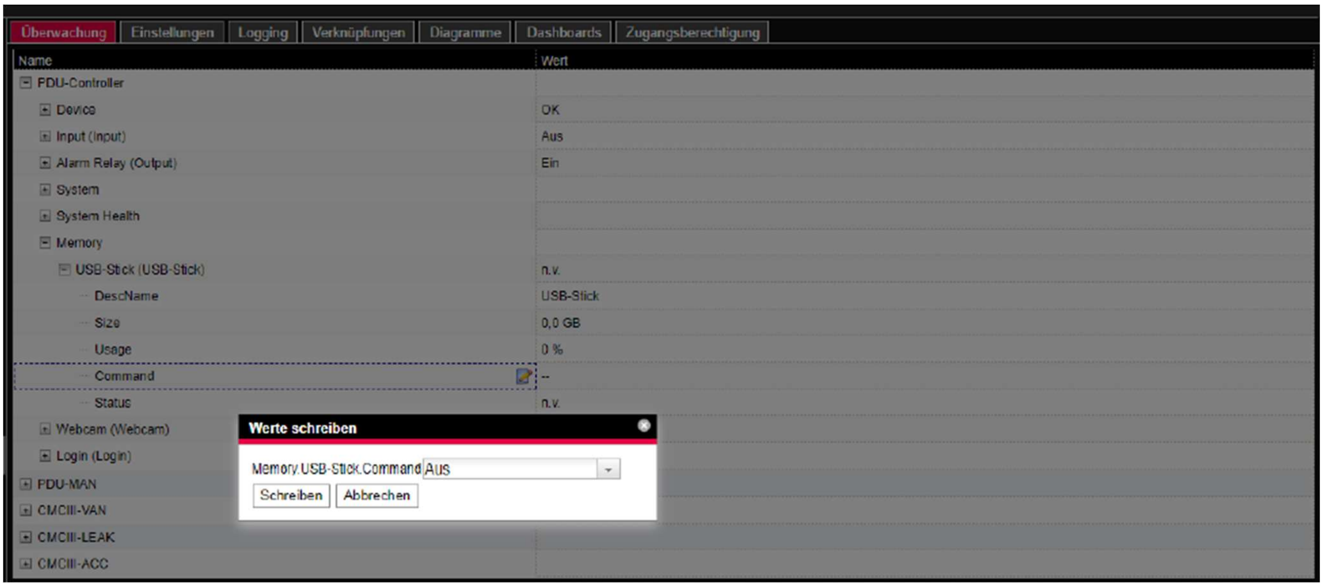
Ensure that the latest Rittal firmware is used on all devices. The firmware can be downloaded from

available for download on the respective product pages on the Internet.

## 4.3 Interfaces

Although the device only accepts and processes known and signed data from the device, it is recommended to deactivate the interfaces (e.g. USB).

This is done in the Monitoring area and the setting can then be found in the device menu under "Memory". The corresponding "Command" for switching off the USB interface ("Off") can be written there.



| Name | Wert |
|---|---|
| PDU-Controller | |
| Device | OK |
| Input (Input) | Aus |
| Alarm Relay (Output) | Ein |
| System | |
| System Health | |
| Memory | |
| USB-Stick (USB-Stick) | n.v. |
| DescName | USB-Stick |
| Size | 0,0 GB |
| Usage | 0 % |
| Command | -- |
| Status | n.v. |
| Webcam (Webcam) | |
| Login (Login) | |
| PDU-MAN | |
| CMCIII-VAN | |
| CMCIII-LEAK | |
| CMCIII-ACC | |

Memory.USB-Stick.Command Aus

Picture 8: USB-Stick configuration

# 5 Access authorization

Unused user accounts must be deactivated.

Where possible, the use of central user administrations for user management and login information is recommended.

## 5.1 Admin permissions

Please note that users who belong to a group with an activated admin flag have access to the complete device configuration via the web management interface and can download and edit all settings.

The number of users with admin authorizations or admin group membership must be limited to the necessary trustworthy persons.

## 5.2 Filetransfer permissions

Users for whom file transfer is permitted can access all data stored on the device and, if write access is enabled, can also change it. This also includes status information and the device configuration. This is independent of membership of a group with an activated admin flag.

File transfer should therefore only be activated for users who are members of a group with an admin flag and, if possible, write access should not be used. Users with file transfer authorization are to be regarded as administrators.

## 5.3 Secure passwords

Do not use standard passwords, but only secure, long passwords that contain numbers, upper/lower case letters, characters and no repetitions.

If possible, create random passwords with a password manager.

## 5.4 Remote access

When using remote access, a secure access method such as VPN (Virtual Private Network) or HTTPS must be selected.

# 6 Factory reset

The following steps are required to reset the device and delete all data and settings:

- Disconnect the device from the power supply.
- Press and hold the display button under the R of the Rittal imprint

- Supply the device with power and keep the button pressed until the status LED turns red.
- Execution of the recovery can be recognized by the white flashing of the status LED.

# Notizen

# 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