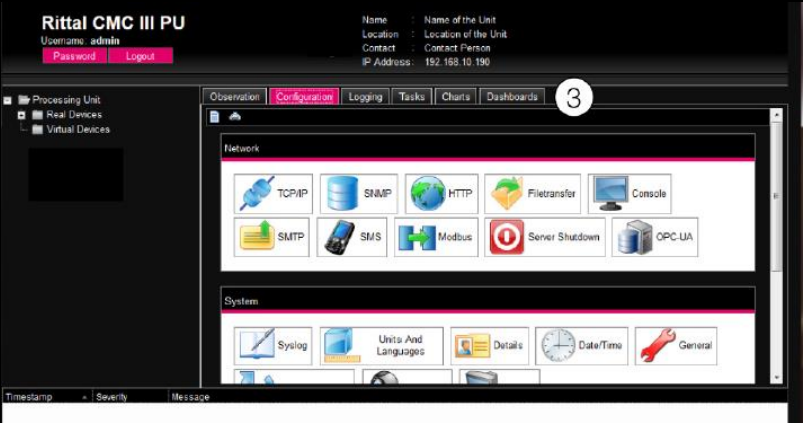


Rittal – The System.

Faster – better – everywhere.



Rittal Embedded Software Devices

System Hardening Guide

Table of contents

1	Introduction.....	3
2	General Information.....	3
3	Channels of communication.....	4
3.1	HTTP (Web-Access)	4
3.2	File Transfer.....	5
3.3	Console.....	5
3.4	SMTP	6
3.5	SNMP	6
3.6	Modbus/TCP	6
3.7	OPC-UA.....	7
3.8	Digital I/O	7
4	File exchange and updates	8
4.1	Security Software	8
4.2	Firmware Version	8
4.3	Interfaces	8
5	Access authorization	9
5.1	Admin permissions	10
5.2	Filetransfer permissions	10
5.3	Secure passwords.....	10
5.4	Remote access.....	10
6	Factory reset.....	10

1 Introduction

Products, networks and systems must be protected against unauthorized access 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-Grundschatz/IT-Grundschatz-Kompendium/it-grundschatz-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.
- Any interfaces, for example the USB ports, shall not be routed or extended outside the secure control cabinet.

3 Channels of communication

Generally, 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. For some protocols, security can be increased by making further settings.

In Order to find sufficient hardening measures for the device it might be helpful to have an overview of all available management protocols and interfaces, which could be targets for attackers.

Interface	Intended Internet Access	Encryption supported
HTTP	NO	NO
HTTPS	NO	YES
SNMP	NO	YES
Modbus TCP	NO	NO
OPC UA	NO	YES
RS232 / RS485	NO	NO
Rittal Sensor Bus (CAN)	NO	NO
USB (Mass- storage&serial)	NO	NO
Digital I/O	NO	NO
Physical buttons	NO	NO

Tabel 1

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 Configuration

Standard Access (without SSL)

Port

Enable ☒

Secure Access (with SSL)

SSL Port

Enable SSL ☒

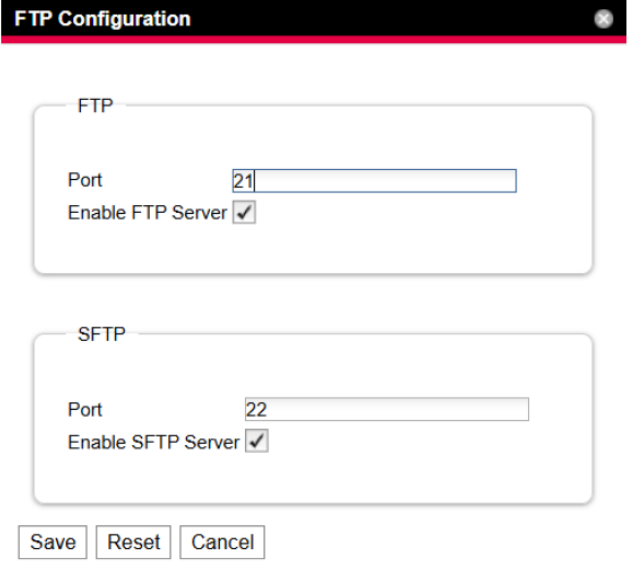
Security Level

Warning: HTTP is enabled. For security reasons, you should only allow HTTPS.

Picture 1: HTTP Settings

3.2 File Transfer

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

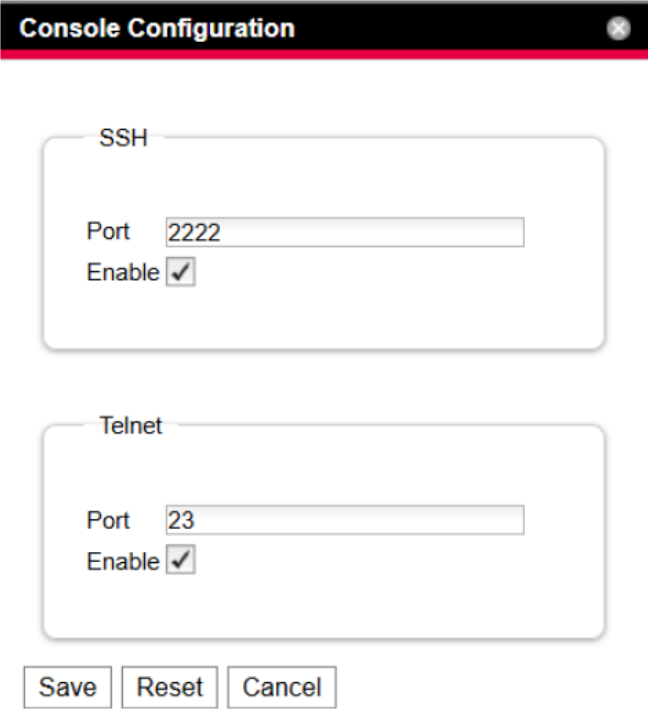


The screenshot shows a dialog box titled "FTP Configuration" with a close button in the top right corner. It contains two sections: "FTP" and "SFTP". The "FTP" section has a "Port" field with the value "21" and an "Enable FTP Server" checkbox that is checked. The "SFTP" section has a "Port" field with the value "22" and an "Enable SFTP Server" checkbox that is checked. At the bottom of the dialog are three buttons: "Save", "Reset", and "Cancel".

Picture 2: File transfer settings

3.3 Console

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



The screenshot shows a dialog box titled "Console Configuration" with a close button in the top right corner. It contains two sections: "SSH" and "Telnet". The "SSH" section has a "Port" field with the value "2222" and an "Enable" checkbox that is checked. The "Telnet" section has a "Port" field with the value "23" and an "Enable" checkbox that is checked. At the bottom of the dialog are three buttons: "Save", "Reset", and "Cancel".

Picture 3: Console settings

3 Channels of communication

EN

3.4 SMTP

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

SMTP Configuration

Server Parameters

Server: smtp.mail.de
Port: 25
Authentication: Yes / TLS
Username: testUser
Password: *****
Sender Address: 10.201.89.12@rittal.com
Reply to Address:

Email

Send device messages: ☐

No.	Email address	Use
1		☐
2		☐
3		☐
4		☐
5		☐
6		☐

Save Reset Cancel

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.

SNMP Configuration

Traps

Enable Authentication Trap: ☐

No.	Trap Receivers	Use
1	SNMPv1 Trap	☐
2	SNMPv1 Trap	☐
3	SNMPv1 Trap	☐
4	SNMPv1 Trap	☐
5	SNMPv1 Trap	☐

SNMPv1/v2c

Enable: ☒
Read Community: public
Write Community: rital
Trap Community: public

Allowed Hosts

No.	Host	Use
1	10.201.89.10	☐
2		☐
3		☐
4		☐

SNMPv3

Enable: ☒
Authentication: SHA
Privacy: AES
SNMPv3 Username: snmp_user
SNMPv3 Password: *****

Save Reset Cancel

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.

Modbus Configuration

Service Parameters

Enable ☐

Port

Allowed Hosts

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

Save

Reset

Cancel

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.

OPC-UA Configuration

OPC-UA Configuration

Enable ☒

Port

Security

Save

Reset

Cancel

Picture 7: OPC-UA configuration

3.8 Digital I/O

The device offers the capability of monitoring and controlling digital I/O over master protocols and tasks. In return tasks can be configured by empowered users to manipulate system states and outputs to master systems. Also, critical system states could be retrieved if a task is configured to switch the alarm relay accordingly.

4 File exchange and updates

EN

Name	Value
PDU-Controller	
Device	OK
Input (Input)	Off
DescName	Input
Value	0
Logic	0:Off / 1:On
Delay	1,0 s
Status	Off
Alarm Relay (Output)	Off
DescName	Alarm Relay
Relay	Off
Logic	0:Off / 1:On
Status	Off
System	

Picture 8: Configuration of digital inputs and outputs

Hence particular care must be taken where signal sources and sinks of digital I/O are placed. In addition, tasks and automations on master systems shall be configured carefully.

Monitoring	Configuration	Logging	Tasks	Charts	Dashboards	Access Configuration
ID	Name	Description	Enabled			
1	Button monitoring	Switch off server if button has been pressed	Yes			
2	Task 2		No			
3	Task 3		No			

Picture 9: Task configuration on the Rittal device

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.

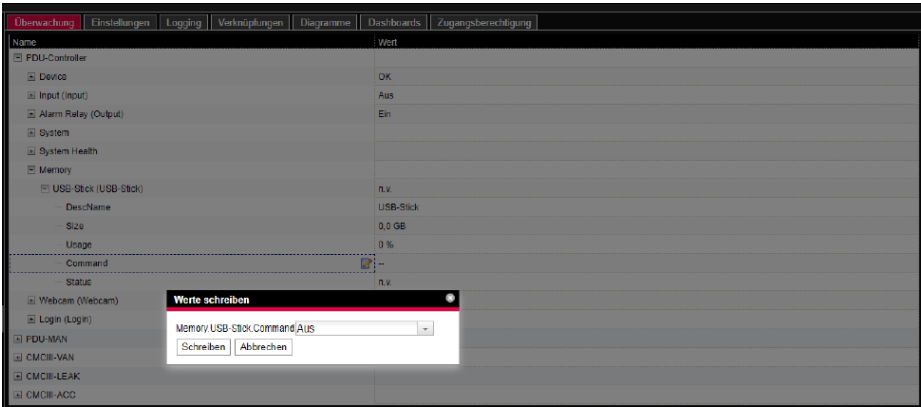
4.2 Firmware Version

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.



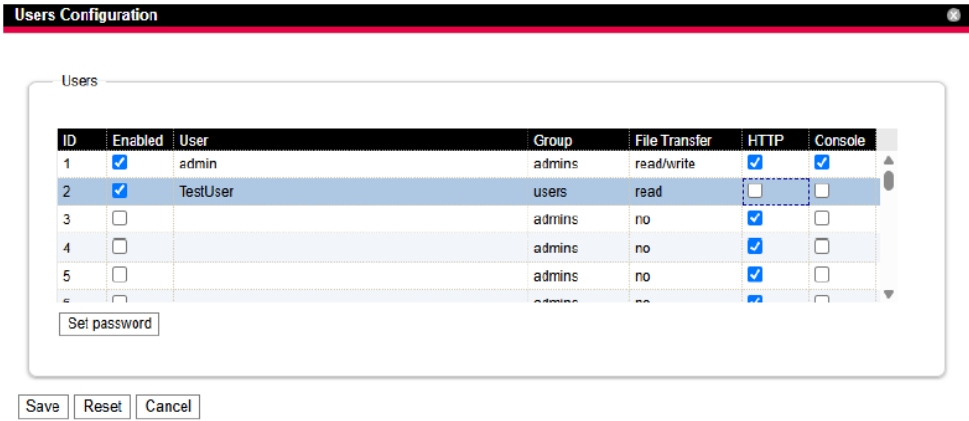
Picture 10: USB-Stick configuration

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. Rittal products support LDAP and RADIUS in this regard.

The local user database on each device is grouped into user groups. For groups and users permissions can be set that will affect the web management interface and general access to the devices protocols.

In user configuration empowered users can enable accounts and give permission for file transfer protocols (FTP & SFTP), grant access to the web management interface (both HTTP & HTTPS) and manage permissions for using the serial console (SSH, Telnet & USB-Serial).

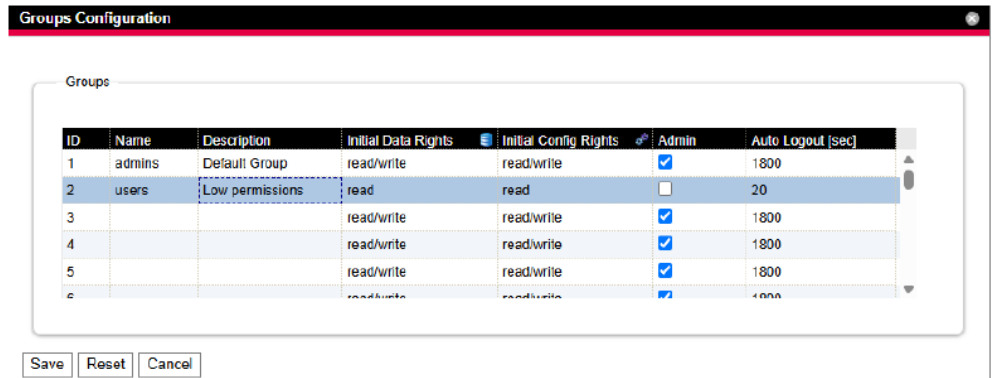


Picture 11: User configuration

User will be assigned to user groups. In the group configuration web management interface timeout and permissions on sensors can be managed according to the products manual.

6 Factory reset

EN



Picture 12: Group configuration

As shown in the screenshots an empowered user can create admin accounts with high permission, but also accounts which have limited access to the product.

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.

Password should be updated after a certain amount of time. The Rittal products will not give feedback on how old a user password is. The responsibility lies on the monitoring system or an external account provider like LDAP or RADIUS server.

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.

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

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

