

Rittal – The System.

Faster – better – everywhere.



Rittal Embedded Software Devices

System Hardening Guide

Inhaltsverzeichnis

1	Einführung	3
2	Generelle Informationen.....	3
3	Kommunikationskanäle.....	4
3.1	HTTP (Web-Access)	4
3.2	File Transfer.....	5
3.3	Konsole.....	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 und Updates	8
4.1	Sicherheits Software	8
4.2	Firmware Version	8
4.3	Schnittstellen.....	8
5	Zugriffsberechtigung	9
5.1	Administratorberechtigung.....	10
5.2	Datenübertragungsberechtigung.....	10
5.3	Sichere Passwörter	10
5.4	Fernzugriff	10
6	Werksreset	10

1 Einführung

Produkte, Netzwerke und Systeme müssen vor unbefugtem Zugriff geschützt werden, um die Verfügbarkeit, Vertraulichkeit und Integrität von Daten zu gewährleisten.

Dies muss durch organisatorische und technische Maßnahmen umgesetzt werden. Rittal empfiehlt bei erhöhtem Sicherheitsbedarf folgende Maßnahmen.

Es gibt nicht nur Informationen zur sicheren Nutzung, sondern auch zu spezifischen Einstellungen am Gerät, die die Sicherheit erhöhen.

In der Praxis muss immer abgewogen werden, inwieweit eine der beschriebenen Änderungen angewendet werden soll oder nicht.

Die verfügbaren Einstellungen können je nach verwendetem Gerät variieren.

Weitere Informationen finden Sie auch auf der Website des Bundesamtes 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 Generelle Informationen

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 geschützt sind.
- Beschränken Sie die Zugriffsberechtigungen auf die Geräte auf Personen, die diese Berechtigung unbedingt benötigen.
- Treffen Sie geeignete Maßnahmen, um den physischen Zugriff auf die Geräte einzuschränken.

3 Kommunikationskanäle

Deaktivieren Sie grundsätzlich alle ungenutzten Kommunikationskanäle auf dem Gerät.

Für viele Protokolle stehen zudem Alternativen mit höherer Sicherheit zur Verfügung. Wir empfehlen, die unsichere Variante zu deaktivieren. Bei einigen Protokollen lässt sich die Sicherheit durch weitere Einstellungen erhöhen.

Um ausreichende Sicherheitsmaßnahmen für das Gerät zu finden, kann es hilfreich sein, einen Überblick über alle verfügbaren Kommunikationswege und Schnittstellen zu haben, die Ziele für Angreifer sein könnten.

Interface	Internetzugriff beabsichtigt	Verschlüsselung unterstützt
HTTP	NEIN	NEIN
HTTPS	NEIN	JA
SNMP	NEIN	JA
Modbus TCP	NEIN	NEIN
OPC UA	NEIN	JA
RS232 / RS485	NEIN	NEIN
Rittal Sensor Bus (CAN)	NEIN	NEIN
USB (Massenspeicher)	NEIN	NEIN
Digital I/O	NEIN	NEIN
Physikalische Taster	NEIN	NEIN

Tabelle 1

3.1 HTTP (Web-Access)

Die Webseite des Gerätes darf nur über HTTPS aufgerufen werden. Es wird empfohlen, die "Sicherheitsstufe" auf "Modern" zu setzen, um die Verwendung von TLS 1.3 zu erzwingen.

HTTP Configuration

Standard Access (without SSL)

Port

Enable ☒

Secure Access (with SSL)

SSL Port

Enable SSL ☒

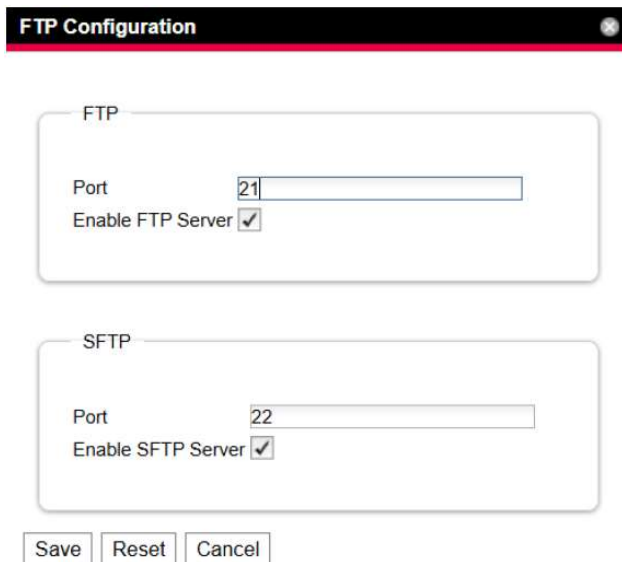
Security Level

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

Bild 1: HTTP-Einstellungen

3.2 File Transfer

Der Zugriff auf das Gerät über FTP/SFTP sollte deaktiviert werden. Der SFTP-Zugriff sollte nur für die Dauer einer Aufgabe (z.B. Software-Update oder Datensicherung) aktiviert werden.



The screenshot shows a window titled "FTP Configuration" with a close button in the top right corner. It contains two sections: "FTP" and "SFTP".

FTP Section:

- Port: 21
- Enable FTP Server: ☒

SFTP Section:

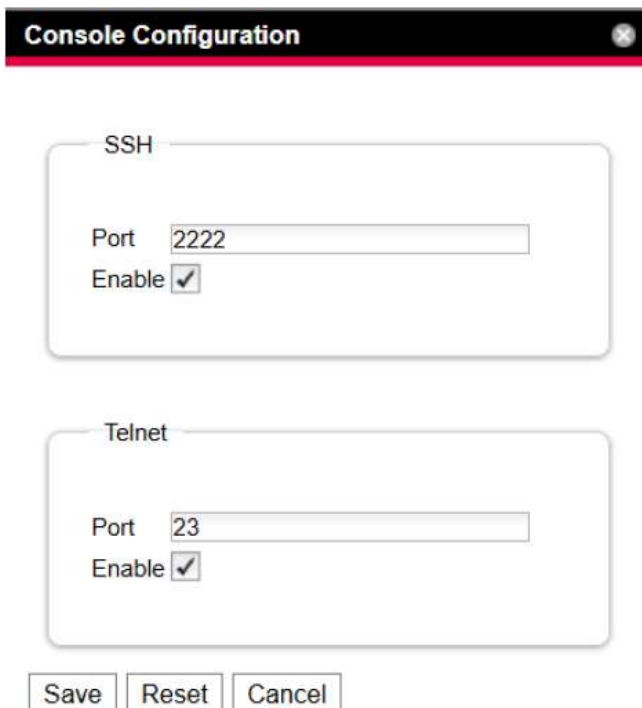
- Port: 22
- Enable SFTP Server: ☒

At the bottom of the window are three buttons: "Save", "Reset", and "Cancel".

Bild 2: File Transfer Einstellungen

3.3 Konsole

Es wird empfohlen, den Konsolenzugriff über Telnet vollständig zu deaktivieren, da die Übertragung unverschlüsselt erfolgt.



The screenshot shows a window titled "Console Configuration" with a close button in the top right corner. It contains two sections: "SSH" and "Telnet".

SSH Section:

- Port: 2222
- Enable: ☒

Telnet Section:

- Port: 23
- Enable: ☒

At the bottom of the window are three buttons: "Save", "Reset", and "Cancel".

Bild 3: Konsolen Einstellungen

3.4 SMTP

Beachten Sie bei der Verwendung von SMTP, dass der verwendete Mailserver eine Authentifizierung und Verschlüsselung unterstützen muss.

SMTP Configuration

Server Parameters

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

Email

Send device messages: ☐

No.	Email address	Use
1		<input type="checkbox"/>
2		<input type="checkbox"/>
3		<input type="checkbox"/>
4		<input type="checkbox"/>
5		<input type="checkbox"/>
6		<input type="checkbox"/>

Save Reset Cancel

Bild 4: SMTP-Einstellungen

3.5 SNMP

Achten Sie bei der Verwendung von SNMP darauf, ausschließlich Version 3 zu verwenden, da die Versionen 1 und 2 keine Authentifizierungs- und Verschlüsselungsmöglichkeiten bieten.

Es wird empfohlen, in den Einstellungen die Authentifizierungsmethode auf SHA und den Datenschutz auf AES einzustellen. Zusätzlich müssen die Standard-Communitys "public" für SNMP überschrieben werden.

Aktuell wird für SNMP auf dem Gerät nur SHA1 unterstützt; falls dies nicht den Anforderungen in der Anwendung/Umgebung entspricht, darf SNMP nicht verwendet werden.

Achten Sie bei der Passwortvergabe darauf, dass dieses den im Abschnitt "Sichere Passwörter" aufgeführten Regeln entspricht. Es wird außerdem empfohlen, im Abschnitt "Erlaubte Hosts" alle Hosts einzutragen, die per SNMP auf das Gerät zugreifen dürfen.

SNMP Configuration

Traps

Enable Authentication Trap: ☐

No.	Trap Receivers	Use
1	SNMPv1 Trap	<input type="checkbox"/>
2	SNMPv1 Trap	<input type="checkbox"/>
3	SNMPv1 Trap	<input type="checkbox"/>
4	SNMPv1 Trap	<input type="checkbox"/>
5	SNMPv1 Trap	<input type="checkbox"/>

SNMPv1/v2c

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

Allowed Hosts

No.	Host	Use
1	10.201.89.10	<input type="checkbox"/>
2		<input type="checkbox"/>
3		<input type="checkbox"/>
4		<input type="checkbox"/>

SNMPv3

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

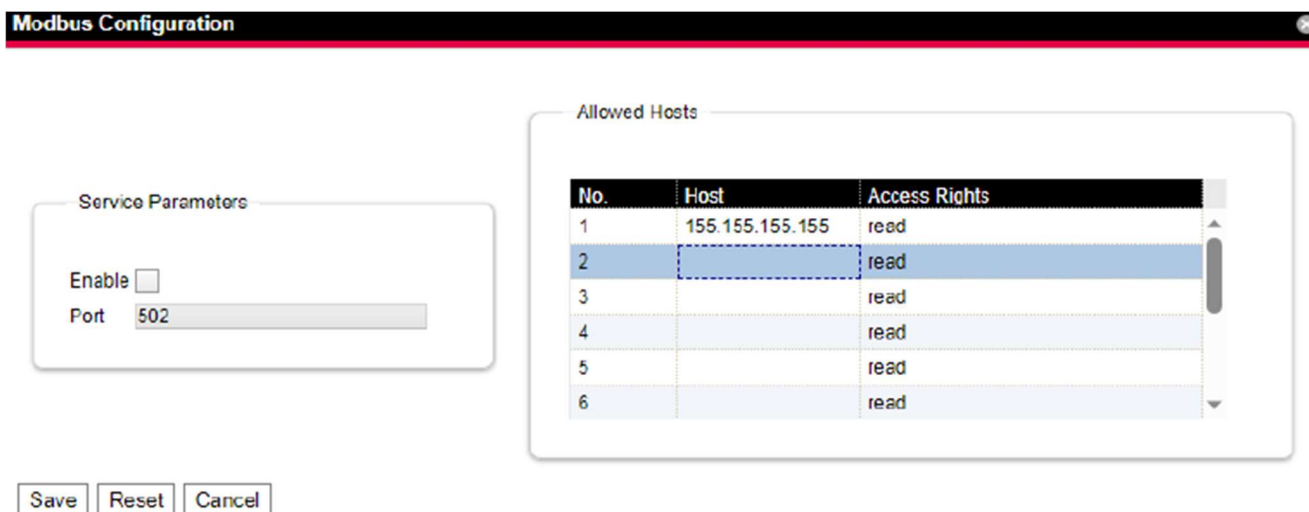
Save Reset Cancel

Bild 5: SNMP-Einstellungen

3.6 Modbus/TCP

Das Modbus-Protokoll bietet keine Authentifizierungs- und Verschlüsselungsfunktion und wird daher nicht empfohlen.

Falls sich der Einsatz nicht vermeiden lässt, empfiehlt es sich, im Bereich "Erlaubte Hosts" die Hosts einzutragen, die über Modbus auf das Gerät zugreifen dürfen. Zudem empfiehlt es sich, den Zugriff möglichst auf "Lesezugriff" zu beschränken.



The **Modbus Configuration** dialog box contains two main sections:

- Service Parameters:**
 - Enable:** An unchecked checkbox.
 - Port:** A text field containing the value **502**.
- Allowed Hosts:** A table with three columns: **No.**, **Host**, and **Access Rights**.

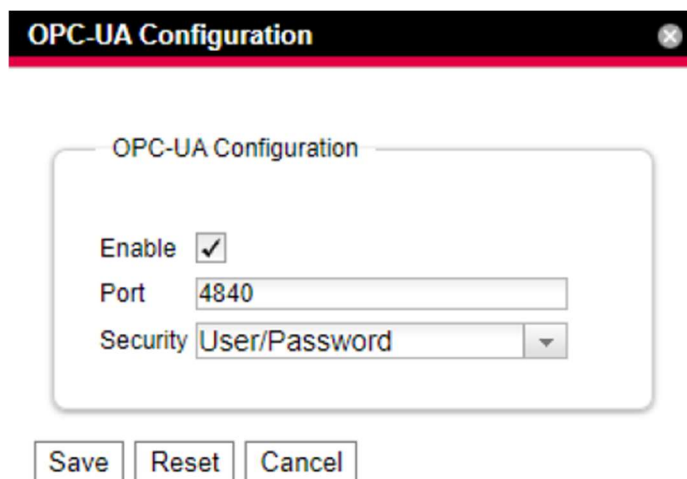
No.	Host	Access Rights
1	155.155.155.155	read
2		read
3		read
4		read
5		read
6		read

At the bottom of the dialog are three buttons: **Save**, **Reset**, and **Cancel**.

Bild 6: Modbus Konfiguration

3.7 OPC-UA

Die Geräte bieten aktuell keine Möglichkeit, den Zugriff über OPC-UA zu verschlüsseln. Sollte OPC-UA dennoch benötigt werden, empfehlen wir, die Benutzerauthentifizierung im Dropdown-Menü „Sicherheit“ einzuschalten und ein sicheres Passwort zu vergeben.



The **OPC-UA Configuration** dialog box contains the following settings:

- Enable:** A checked checkbox.
- Port:** A text field containing the value **4840**.
- Security:** A dropdown menu currently showing **User/Password**.

At the bottom of the dialog are three buttons: **Save**, **Reset**, and **Cancel**.

Bild 7: OPC-UA Konfiguration

3.8 Digital I/O

Das Gerät bietet die Möglichkeit, digitale Ein- und Ausgänge über Master-Protokolle und Tasks zu überwachen und zu steuern. Im Gegenzug können Tasks von berechtigten Benutzern konfiguriert werden, um Systemzustände und Ausgänge an Master-Systemen zu manipulieren. Kritische Systemzustände können außerdem abgerufen werden, wenn eine Aufgabe konfiguriert ist, die das Alarmrelais entsprechend schaltet.

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	

Bild 8: Konfiguration der digitalen Ein- und Ausgänge

Daher muss besonders darauf geachtet werden, wo Signalquellen und -senken digitaler E/A platziert werden. Darüber hinaus müssen Aufgaben und Automatisierungen auf Mastersystemen sorgfältig konfiguriert werden.

	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				

Bild 9: Aufgaben Konfiguration auf einem Rittal Gerät

4 File exchange und Updates

4.1 Sicherheitssoftware

Um Sicherheitsrisiken wie Viren, Trojaner und andere Schadsoftware zu erkennen und zu beseitigen, empfiehlt es sich, auf allen PCs Sicherheitssoftware zu installieren und diese auf dem neuesten Stand zu halten.

Alle auf das Gerät hochgeladenen Daten müssen vom Benutzer überprüft werden.

4.2 Firmware Version

Stellen Sie sicher, dass auf allen Geräten die neueste Rittal-Firmware verwendet wird. Die Firmware steht auf den jeweiligen Produktseiten auf der Rittal-Website zum Download bereit.

4.3 Schnittstellen

Obwohl das Gerät nur bekannte und signierte Daten akzeptiert und verarbeitet, empfiehlt es sich die Schnittstellen (z.B. USB) zu deaktivieren.

Dies geschieht im Bereich Monitoring. Die Einstellung ist anschließend im Gerätemenü unter "Speicher" zu finden. Dort kann der entsprechende "Befehl" zum Abschalten der USB-Schnittstelle eingetragen werden.

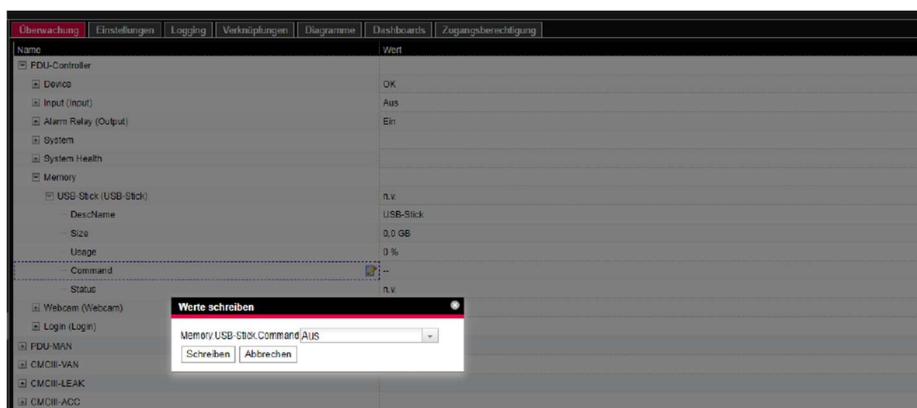


Bild 10: USB-Stick Konfiguration

5 Zugriffsberechtigung

Nicht genutzte Benutzerkonten müssen deaktiviert werden.

Wir empfehlen nach Möglichkeit die Nutzung zentraler Benutzerverwaltung und Anmeldeinformationen. Rittal-Produkte unterstützen hierfür LDAP und RADIUS.

Die lokale Benutzerdatenbank jedes Gerätes ist in Benutzergruppen eingeteilt. Für Gruppen und Benutzer lassen sich Berechtigungen festlegen, die sich auf die Web-Oberfläche und den allgemeinen Zugriff auf die Geräteprotokolle auswirken.

In der Benutzerkonfiguration können berechtigte Benutzer Konten aktivieren und Berechtigungen für Dateiübertragungsprotokolle (FTP und SFTP) erteilen, Zugriff auf die Web-Oberfläche (sowohl HTTP als auch HTTPS) gewähren und Berechtigungen für die Verwendung der seriellen Konsole (SSH, Telnet und USB) verwalten.

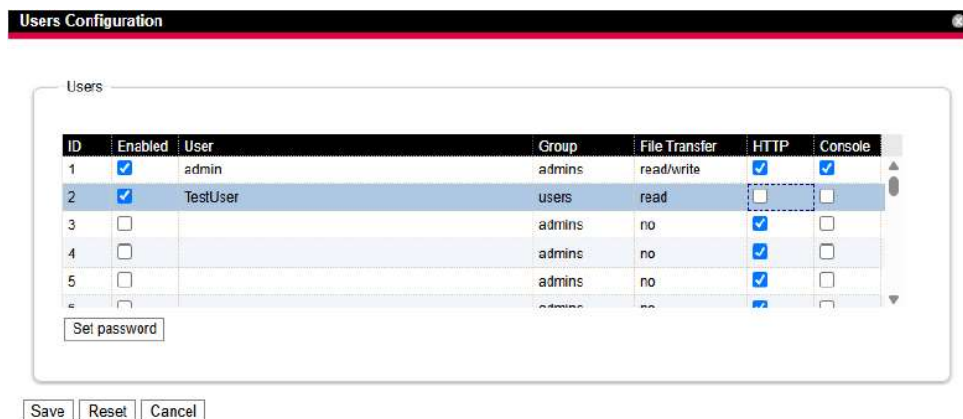


Bild 11: Benutzer Konfiguration

Benutzer werden Benutzergruppen zugewiesen. In der Gruppenkonfiguration der Web-Oberfläche können Timeout und Berechtigungen für Sensoren gemäß dem Produkthandbuch verwaltet werden.

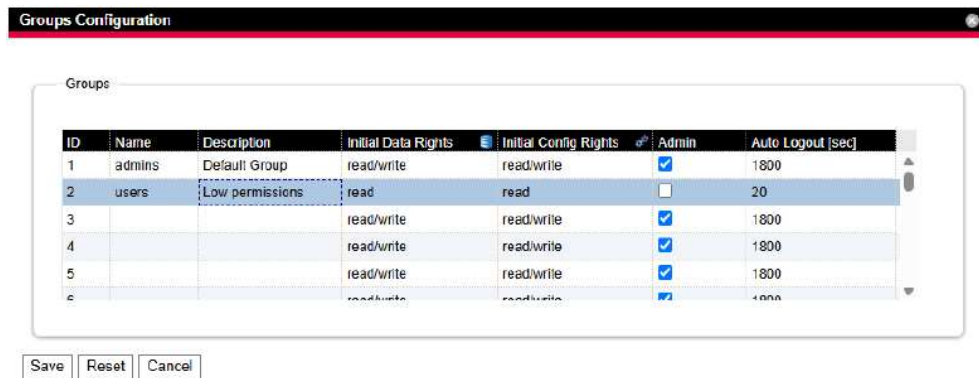


Bild 12: Gruppen Konfiguration

Wie in den Screenshots gezeigt, kann ein berechtigter Benutzer Administratorenkonten mit hohen Berechtigungen erstellen, aber auch Konten mit eingeschränktem Zugriff.

5.1 Administratorberechtigung

Bitte beachten Sie, dass Benutzer, die einer Gruppe mit aktiviertem Admin-Flag angehören, über die Web-Oberfläche Zugriff auf die komplette Gerätekonfiguration haben und alle Einstellungen herunterladen und bearbeiten können. Die Anzahl der Benutzer mit Admin-Berechtigung muss auf die notwendigen vertrauenswürdigen Personen beschränkt werden.

5.2 Datenübertragungsberechtigung

Benutzer mit der Berechtigung zum Datentransfer können auf alle auf dem Gerät gespeicherten Daten zugreifen und diese bei aktiviertem Schreibzugriff auch ändern. Dies umfasst auch Statusinformationen und die Gerätekonfiguration. Dies ist unabhängig von der Mitgliedschaft in einer Gruppe mit aktiviertem Admin-Flag. Der Dateitransfer sollte daher nur für Benutzer aktiviert werden, die Mitglied einer Gruppe mit Admin-Flag sind und wenn möglich sollte kein Schreibzugriff verwendet werden. Benutzer mit Dateitransferberechtigung sind als Administratoren anzusehen.

5.3 Sichere Passwörter

Verwenden Sie keine Standardpasswörter, sondern nur sichere, lange Passwörter, die Zahlen, Groß- und Kleinbuchstaben, Sonderzeichen und keine Wiederholungen enthalten.

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

Passwörter sollten nach einer bestimmten Zeit aktualisiert werden. Rittal Produkte geben keine Rückmeldung zum Alter eines Benutzerpassworts. Die Verantwortung liegt beim Überwachungssystem oder einem externen Account-Provider wie einem LDAP oder RADIUS Server.

5.4 Fernzugriff

Bei der Nutzung des Fernzugriffs muss eine sichere Zugriffsmethode wie VPN (Virtual Private Network) oder HTTPS ausgewählt werden.

6 Werksreset

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

- Trennen Sie das Gerät von der Stromversorgung
- Halten Sie die Displaytaste unter dem "R" des Rittal-Schriftzuges gedrückt.

- Versorgen Sie das Gerät wieder mit Strom und halten Sie die Taste weiter gedrückt, bis die Status LED rot leuchtet
- Die Durchführung der Wiederherstellung erkennen Sie am weißen Blinken 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

ENCLOSURES

POWER DISTRIBUTION

CLIMATE CONTROL

IT INFRASTRUCTURE

SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

