Rittal – The System.

Faster – better – everywhere.

DK Access Control

7010.180

Montage-, Installations- und Bedienungsanleitung

DE

Vorwort

Sehr geehrter Kunde!

Vielen Dank, dass Sie sich für einen Access Control aus unserem Hause entschieden haben!

Viel Erfolg wünscht Ihnen

Ihre
Rittal GmbH & Co. KG

Rittal GmbH & Co. KG
Auf dem Stuetzelberg

35745 Herborn
Germany

Tel.: +49(0)2772 505-0
Fax: +49(0)2772 505-2319

E-Mail: info@rittal.de
www.rittal.com
www.rittal.de

Wir stehen Ihnen zu technischen Fragen rund um unser Produktspektrum zur Verfügung.

DE

Inhaltsverzeichnis

DE

1 Hinweise zur Dokumentation

1.1 CE-Kennzeichnung

Rittal GmbH & Co. KG bestätigt die Konformität des Access Control zur EG-EMV-Richtlinie 2014/30/EU. Eine entsprechende Konformitätserklärung wurde ausgestellt. Sie kann auf Anforderung vorgelegt werden.

CE

1.2 Aufbewahrung der Unterlagen

Die Montage-, Installations- und Bedienungsanleitung sowie alle mitgeltenden Unterlagen sind ein integraler Bestandteil des Produkts. Sie müssen den mit dem Gerät befassten Personen ausgehändigt werden und müssen stets griffbereit und für das Bedienungs- und Wartungspersonal jederzeit verfügbar sein!

1.3 Symbole in dieser Betriebsanleitung

Folgende Symbole finden Sie in dieser Dokumentation:

Gefahr!
Gefährliche Situation, die bei Nichtbeachtung des Hinweises unmittelbar zu Tod oder schwerer Verletzung führt.

Warnung!
Gefährliche Situation, die bei Nichtbeachtung des Hinweises unmittelbar zu Tod oder schwerer Verletzung führen kann.

Vorsicht!
Gefährliche Situation, die bei Nichtbeachtung des Hinweises zu (leichten) Verletzungen führen kann.

Hinweis:
Kennzeichnung von Situationen, die zu Sachschäden führen können.

- Dieses Symbol kennzeichnet einen „Aktionspunkt“ und zeigt an, dass Sie eine Handlung bzw. einen Arbeitsschritt durchführen sollen.

1.4 Mitgeltende Unterlagen

– Installations- und Kurz-Bedienungsanleitung
– Montage-, Installations- und Bedienungsanleitung des verwendeten Rittal Embedded Device

1.5 Geltungsbereich

In der vorliegenden Dokumentation werden durchgängig englische Screenshots gezeigt. Auch in den Beschreibungen zu den einzelnen Parametern auf der Website des Rittal Embedded Device werden die englischen Begriffe verwendet. Je nach eingestellter Sprache können die Anzeigen auf der Website des Rittal Embedded Device hiervon abweichen (siehe Montage-, Installations- und Bedienungsanleitung des verwendeten Rittal Embedded Device).

DE

2 Sicherheitshinweise

2.1 Allgemein gültige Sicherheitshinweise

Bitte beachten Sie die nachfolgenden allgemeinen Sicherheitshinweise bei Installation und Betrieb des Systems:

- Montage und Installation des Access Control dürfen nur durch versiertes Fachpersonal erfolgen.
- Das Gehäuse des Access Control darf nicht geöffnet werden!
- Der Access Control darf nicht in Kontakt mit Wasser, aggressiven oder entzündbaren Gasen und Dämpfen geraten!
- Der Access Control darf nur innerhalb der in den technischen Daten spezifizierten Grenzen betrieben werden!
- Der Access Control darf ausschließlich über den CAN-Bus mit der notwendigen Betriebsspannung versorgt werden.
- Der Access Control darf nicht an Orten verwendet werden, an denen möglicherweise Kinder anwesend sein können.
- Verwenden Sie im Zusammenhang mit dem Access Control ausschließlich Original-Rittal oder von Rittal empfohlene Produkte.
- Nehmen Sie am Access Control keine Änderungen vor, die nicht in dieser oder in den mitgeltenden Montage- und Bedienungsanleitungen beschrieben sind.
- Die Betriebssicherheit des Access Control ist nur bei bestimmungsgemäßer Verwendung gewährleistet. Die technischen Daten und angegebenen Grenzwerte dürfen auf keinen Fall überschritten werden. Dies gilt insbesondere für die spezifizierte Umgebungstemperatur und IP-Schutzart.
- Beachten Sie außer diesen allgemeinen Sicherheitshinweisen unbedingt auch die spezifischen Sicherheitshinweise im Zusammenhang mit den in den folgenden Kapiteln aufgeführten Tätigkeiten.

REACH Sicherheitshinweis gemäß Verordnung (EG) Nr. 1907/2006

- Das Produkt enthält den SVHC-Stoff „Blei – CAS-Nr. 7439-92-1“.
- Lt. Angaben des Herstellers entstehen bei ordnungsgemäßem Umgang mit dem Produkt während des Gebrauchs keinerlei Gesundheitsrisiken.
- Nach Gebrauch muss das Produkt entsprechend der geltenden gesetzlichen Regelungen ordnungsgemäß entsorgt werden.

2.2 Bedien- und Fachpersonal

- Die Montage, Installation, Inbetriebnahme, Wartung und Instandsetzung dieses Gerätes dürfen nur von qualifizierten mechanischen und elektrotechnischen Fachleuten durchgeführt werden.
- Die Gerätebedienung im laufenden Betrieb darf nur eine eingewiesene Person durchführen.

DE

3 Produktbeschreibung

3.1 Funktionsbeschreibung und Bestandteile

3.1.1 Funktion

Der Access Control dient zur Überwachung von Rack-Türen über einen Infrarot-Zugangssensor sowie zur generellen Überwachung bzgl. Erschütterungen. Des Weiteren können an den Schnittstellen ein CMC III-Lesegerät sowie ein Griff angeschlossen werden. Der Zugangssensor meldet, ob die Tür offen oder geschlossen ist. Am Lesegerät werden Codes zur Türfreigabe eingegeben. Mit einem elektrischen Griff kann die Tür dann geöffnet sowie der Türgriff überwacht werden. Der Access Control enthält eine Kennung, durch die er automatisch vom Rittal Embedded Device erkannt wird.

3.1.2 Bestandteile

Das Gerät besteht aus einem kompakten Kunststoffgehäuse in RAL 9005 mit belüfteter Front.

3.2 Bestimmungsgemäße Verwendung, vorhersehbarer Fehlgebrauch

Der Access Control dient ausschließlich zur Zugangsüberwachung an einem Serverschrank sowie zur generellen Überwachung bzgl. Erschütterungen. Er darf nur zusammen mit Rittal Embedded Devices (ab Softwareversion 10.0.0) verwendet werden. Vorgesehene Einsatzorte sind Schränke und Schrank-Anreihungen sowie Rahmengestelle zur Aufnahme von Server- und Netzwerktechnik in Sicherheits- und Technikräumen. Der Access Control darf ausschließlich mit dem von Rittal vorgesehenen Systemzubehör und den von Rittal vorgesehenen Kabeln kombiniert und betrieben werden (siehe Montage-, Installations- und Bedienungsanleitung CMC III Processing Unit – Dokument D-0000-00000553-00). Eine andere Verwendung ist nicht bestimmungsgemäß.

Das Gerät ist nach dem Stand der Technik und den anerkannten sicherheitstechnischen Regeln gebaut. Dennoch können bei nicht ordnungsgemäßer Verwendung Beeinträchtigungen der Anlage und anderer Sachwerte entstehen.

Das Gerät ist daher nur bestimmungsgemäß in technisch einwandfreiem Zustand zu benutzen! Störungen, die die Sicherheit beeinträchtigen können, sollten Sie umgehend beseitigen (lassen)! Betriebsanleitung beachten!

Zur bestimmungsgemäßen Verwendung gehören auch das Beachten der vorliegenden Dokumentation und die Einhaltung der Inspektions- und Wartungsbedingungen.

Für Schäden, die durch Nichtbeachtung der vorliegenden Dokumentation entstehen, übernimmt Rittal GmbH & Co. KG keine Haftung. Dies gilt auch für das Nichtbeachten der gültigen Dokumentationen des verwendeten Zubehörs bzw. der Basissysteme.

Bei nicht bestimmungsgemäßem Gebrauch können Gefahren auftreten. Solch nicht bestimmungsgemäßer Gebrauch kann z. B. sein:

– Verwendung von unzulässigen Werkzeugen.
– Unsachgemäße Bedienung.
– Unsachgemäße Behebung von Störungen.
– Verwendung von nicht durch Rittal GmbH & Co. KG freigegebenem Zubehör.

3.3 Lieferumfang

– Access Control
– Beigelegtes Zubehör (Abb. 1)
– Installations- und Kurz-Bedienungsanleitung

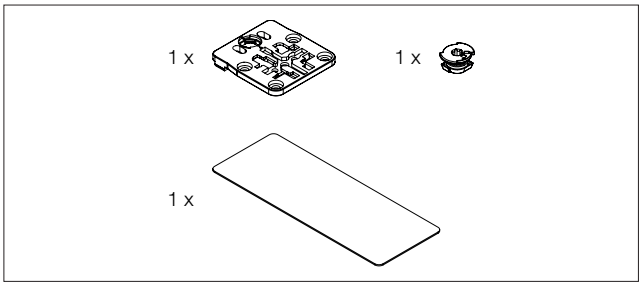


Abb. 1: Beigelegtes Zubehör

DE

4 Transport und Handhabung

4.1 Transport

Das Gerät wird in einem Karton geliefert.

4.2 Auspacken

- Entfernen Sie die Verpackung des Gerätes.

Hinweis:
Die Verpackung muss nach dem Auspacken umweltgerecht entsorgt werden. Sie besteht aus folgenden Materialien:
Poly-Ethylen-Folie (PE-Folie), Karton.

- Prüfen Sie das Gerät auf Transportschäden.

Hinweis:
Schäden und sonstige Mängel, z. B. Unvollständigkeit, sind der Spedition und der Fa. Rittal GmbH & Co. KG unverzüglich schriftlich mitzuteilen.

- Entnehmen Sie das Gerät aus der PE-Folie.
- Entfernen Sie die Schutzfolie von der Frontblende des Gerätes.

DE

5 Installation

5.1 Sicherheitshinweise

- Bitte beachten Sie die zur Installation gültigen Vorschriften des Landes, in dem der Access Control installiert und betrieben wird, sowie dessen nationale Vorschriften zur Unfallverhütung. Bitte beachten Sie außerdem betriebsinterne Vorschriften wie Arbeits-, Betriebs- und Sicherheitsvorschriften.
- Die technischen Daten und angegebenen Grenzwerte dürfen auf keinen Fall überschritten werden. Dies gilt insbesondere für die spezifizierte Umgebungstemperatur und IP-Schutzart.
- Wenn für die spezielle Anwendung eine höhere IP-Schutzart gefordert ist, muss der Access Control in ein entsprechendes Gehäuse bzw. einen entsprechenden Schrank mit der geforderten IP-Schutzart eingebaut werden. Unter Umständen ist dann die Funktion des integrierten Infrarot-Sensors nicht mehr gegeben.

5.2 Anforderungen an den Installationsort

Um eine einwandfreie Funktion des Geräts zu gewährleisten, sind die im Abschnitt 8 „Technische Daten“ genannten Bedingungen für den Installationsort des Geräts zu beachten.

Elektromagnetische Beeinflussung

– Störende Elektroinstallationen (Hochfrequenz) müssen vermieden werden.

5.3 Montageablauf

Generell bestehen mehrere Möglichkeiten, den Access Control zu montieren:

1. Montage mit dem beigelegten Halter am Rahmen des Schaltschranks bzw. IT-Schranks.
2. Montage mit dem beigelegten Halter an einem System-Chassis.
3. Optional: Montage mit dem beigelegtem Halter und zusätzlich mit Federclip (Zubehör) auf einer Hutschiene.

5.3.1 Hinweise zur Montage

- Montieren Sie den Access Control so, dass die Front mit Sender und Empfänger zu der zu überwachenden Tür hin zeigt.
- Montieren Sie den Access Control vorzugsweise so, dass der Infrarot-Zugangssensor auf die Schloss- und nicht auf die Scharnierseite der zu überwachenden Tür zeigt.
  Hier ändert sich der Winkel der Reflexfolie schneller und eine geöffnete Tür wird so schneller erkannt.
- Montieren Sie den Access Control so, dass er ausreichend gut mit Luft durchströmt wird und die Lüftungsschlitze nicht verdeckt werden.
- Kleben Sie die beigelegte Reflexfolie exakt an die dem Infrarot-Zugangssensor gegenüberliegende Position an der Tür.
- Beachten Sie die in der folgenden Tabelle angegebenen Minimal- und Maximalabstände zwischen dem Sensor und der Reflexfolie in Abhängigkeit vom eingestellten Wert für die „Sensitivity“.

Sensitivity	**min. Abstand** mm	**max. Abstand** mm
1	20	70
2	20	100
3	20	130

Tab. 1: Minimale und maximale Abstände

Hinweis:
Im Auslieferungszustand ist die Sensitivity auf den Wert „2“ voreingestellt.

- Stellen Sie sicher, dass die Montage des Access Control ausschließlich in einer der dargestellten Positionen erfolgt.

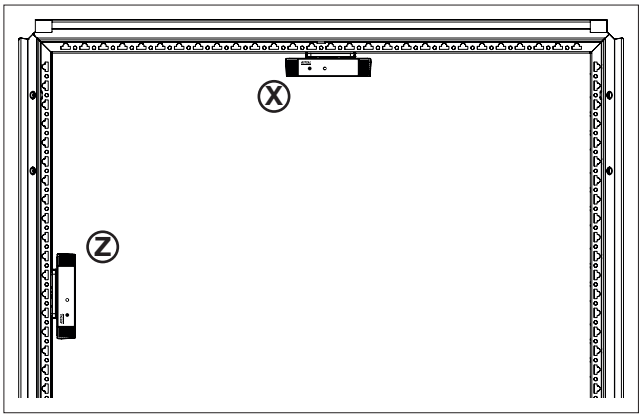


Abb. 2: Montagepositionen

5.3.2 Montage mit dem beigelegten Halter am Schrankrahmen

Die Montage am Rahmen eines IT-Schranks erfolgt mit dem im Lieferumfang beigelegten Halter.

- Knipsen Sie für eine Montage an einem TS IT Schrank die auf der Rückseite überstehenden Nasen am Halter ab.

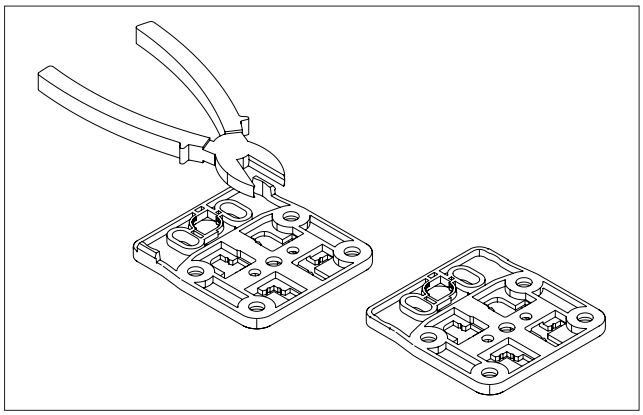


Abb. 3: Vorbereiten des Halters für Montage an einem TS IT Schrank

- Setzen Sie den Access Control von oben auf den Halter auf.

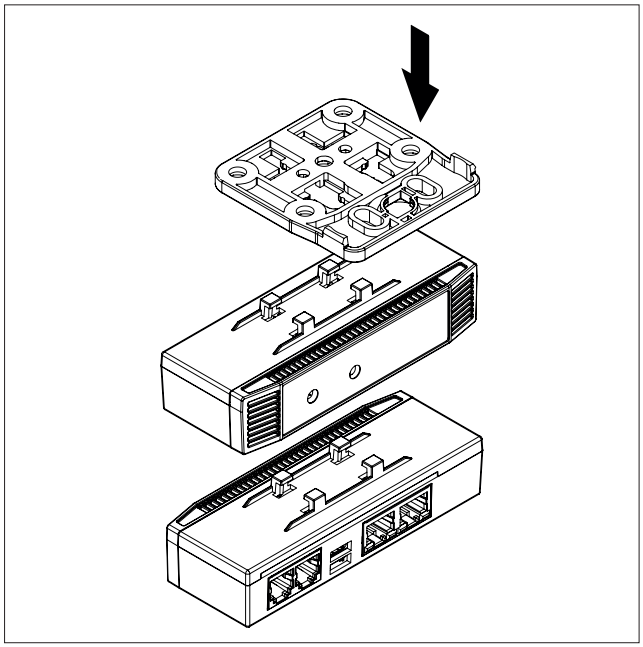


Abb. 4: Aufsetzen des Sensors auf den Halter

- Verschieben Sie den Sensor auf dem Halter leicht seitlich, so dass er einrastet.

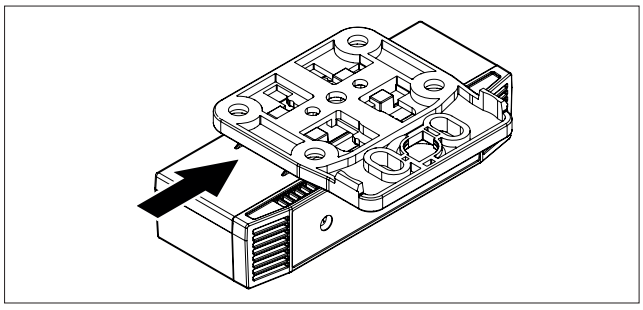


Abb. 5: Einrasten des Sensors auf dem Halter

- Befestigen Sie den Halter inkl. Access Control durch eine Vierteldrehung des Verbinders an der gewünschten Position im Schaltschrank bzw. IT-Schrank.

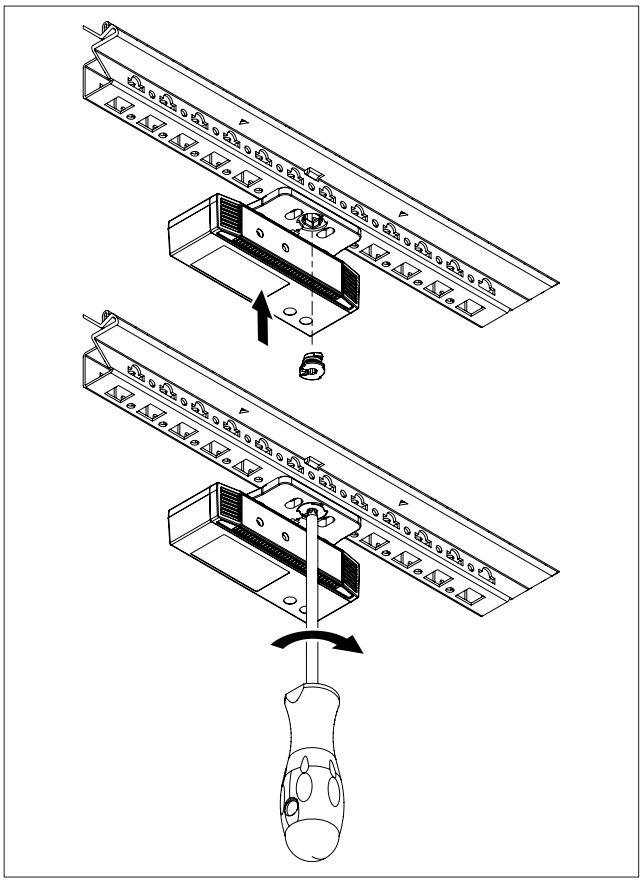


Abb. 6: Montage Schrankprofil „X“

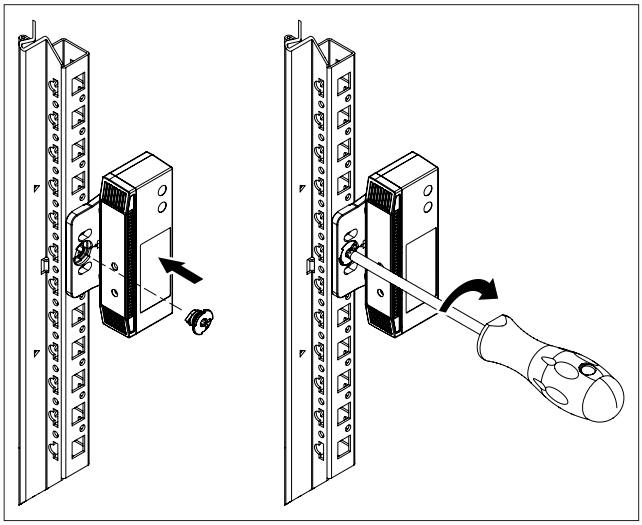


Abb. 7: Montage Schrankprofil „Z“

- Sichern Sie optional den Halter zusätzlich mit zwei Schrauben M5,5 x 13.

DE

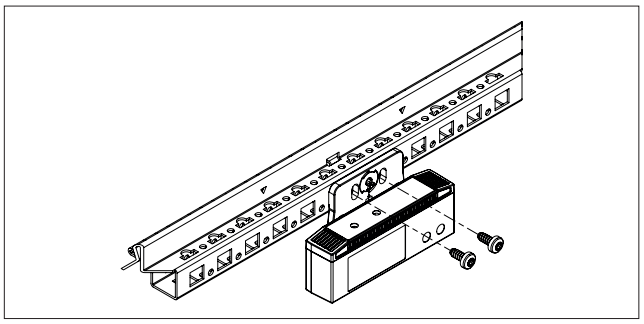


Abb. 8: Optionales Sichern des Halters (Schrankprofil „X“ oder Schrankprofil „Z“)

5.3.3 Montage mit dem beigelegten Halter an einem System-Chassis

Die Montage auf einem System-Chassis erfolgt mit dem im Lieferumfang beigelegten Halter.

- Setzen Sie den Access Control von oben auf den Halter auf und rasten Sie ihn ein, analog wie für eine Montage am Schrankrahmen.
- Befestigen Sie den Halter inkl. Access Control durch eine Vierteldrehung des Verbinders an der gewünschten Position auf dem System-Chassis.

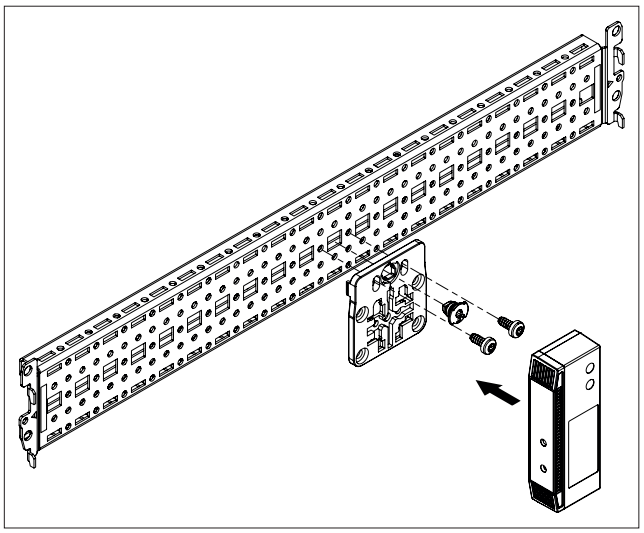


Abb. 9: Befestigen des Sensors auf einem System-Chassis

- Sichern Sie den Halter zusätzlich optional mit zwei Schrauben M5,5 x 13, analog wie bei einer Montage am Schrankrahmen.

5.3.4 Montage auf einer Hutschiene

Für eine Hutschienenmontage wird zusätzlich zum Halter aus dem Lieferumfang ein Federclip benötigt (Zubehör).

- Schrauben Sie zunächst den Halter mit zwei Schrauben M4 x 10 auf den Federclip zur Hutschienenmontage.
- Setzen Sie dann den Access Control auf den Halter auf und rasten Sie ihn ein.

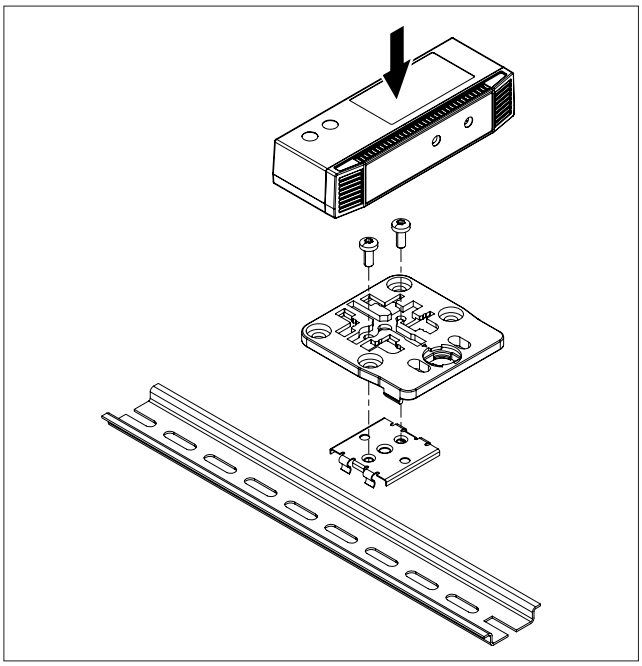


Abb. 10: Befestigen des Halters auf dem Federclip

- Rasten Sie den Federclip an der gewünschten Position auf der Hutschiene auf.

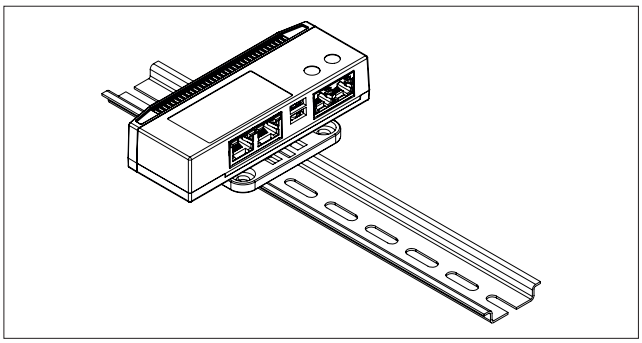


Abb. 11: Sensor mit Federclip auf der Hutschiene

5.4 Anschluss des Sensors

Der Access Control wird über den CAN-Bus-Anschluss mit der notwendigen Betriebsspannung versorgt. Der Anschluss eines separaten Netzteils ist nicht notwendig.

- Schließen Sie ggf. folgendes Anschlusszubehör am entsprechenden Anschluss an (Abb. 12, Pos. 4 bis 7).
  - CMC III Zahlencodeschloss VX (7030.222, 7030.223)
  - CMC III Transponderleser VX (7030.232, 7030.233)
  - CMC III Online-Komfortgriff VX (7030.610, 7030.611)
  - elektromagnetischer Griff Ergoform-S (7320.700)
  - elektromagnetischer TS 8-Griff mit Master-Key-Funktion mit und ohne CCP (7320.721)
- Verbinden Sie den Access Control über ein CAN-Bus-Verbindungskabel mit einer CAN-Bus-Schnittstelle des Rittal Embedded Device bzw. der benachbarten Komponente im CAN-Bus (Abb. 12, Pos. 8, 9).

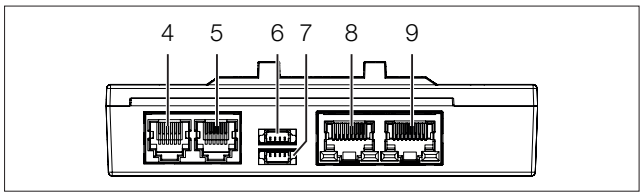


Abb. 12: Rückseite des Access Control

Legende

4 Anschluss für Griff RJ 12
5 Anschluss für Griff RJ 12
6 Anschluss für CMC III Lesegerät
7 Anschluss für CMC III Lesegerät
8 CAN-Bus-Anschluss, 24 V ⎓, 1 A
9 CAN-Bus-Anschluss, 24 V ⎓, 1 A

Folgende CAN-Bus-Verbindungskabel können über Fa. Rittal bezogen werden:

– DK 7030.090 (Länge 0,5 m)
– DK 7030.091 (Länge 1 m)
– DK 7030.092 (Länge 1,5 m)
– DK 7030.093 (Länge 2 m)
– DK 7030.480 (Länge 3 m)
– DK 7030.490 (Länge 4 m)
– DK 7030.094 (Länge 5 m)
– DK 7030.095 (Länge 10 m)

Ggf. wird nach dem Anschluss ein Software-Update des Sensors durchgeführt. Während des gesamten Update-Vorgangs leuchtet die Status-LED des Access Control dauerhaft blau, während der Sensor selbst ein Update erhält.
Außerdem blinkt die Status-LED des Rittal Embedded Device weiß und es erscheint eine entsprechende Meldung auf der Website.

Hinweis:
Solange der Update-Vorgang läuft, können keine Einstellungen vorgenommen werden.

Das Update des Sensors ist vollständig abgeschlossen, wenn folgende Bedingungen erfüllt sind:

1. Die LEDs am Bus-Anschluss des Sensors leuchten grün.
2. Die Multi-LED des Sensors hinter der Frontblende blitzt blau und zusätzlich grün, gelb oder rot, je nach Zustand des Sensors.

Der Anschluss weiterer Komponenten erfolgt als Daisy Chain.

- Beachten Sie beim Anschluss von weiteren Komponenten am CAN-Bus folgende Beschränkungen:
  – Bei der Installation der Sensoren oder anderer kompatibler Komponenten darf der Gesamtstrom pro CAN-Bus-Kanal 1 A nicht überschreiten.
  – Stromverbrauch Access Control: 40 mA zzgl. 125 mA pro angeschlossenem Griff
- Schließen Sie ggf. an der zweiten, freien CAN-Bus-Schnittstelle des Access Control (Abb. 12, Pos. 8, 9) eine weitere Komponente an (z. B. einen anderen Sensortyp).

  Anzeige der Statusänderung:
  – Die beiden grünen sowie die beiden roten CAN-Bus LEDs am CAN-Bus-Anschluss blinken.
  – Die Multi-LED des Rittal Embedded Device blinkt dauerhaft in der Reihenfolge grün – gelb – rot.
  – Die Multi-LED des Access Control blinkt dauerhaft blau.
- Drücken Sie die „C“-Taste am Rittal Embedded Device (ein erster Signalton ertönt) und halten Sie sie für ca. 3 Sekunden gedrückt, bis ein zweiter Signalton ertönt.

Hinweis:
Eine Auflistung aller Anzeigen der Multi-LED finden Sie im Abschnitt 6.3.1 „Anzeigen der Multi-LED“.

DE

6 Bedienung

6.1 Einschalten des Access Control

Nach dem Anschließen des Access Control an eine benachbarte Komponente über ein CAN-Bus-Verbindungskabel startet der Access Control automatisch (vgl. Abschnitt 5.4 „Anschluss des Sensors“). Ein separates Einschalten ist nicht erforderlich.

6.2 Bedien- und Anzeigeelemente

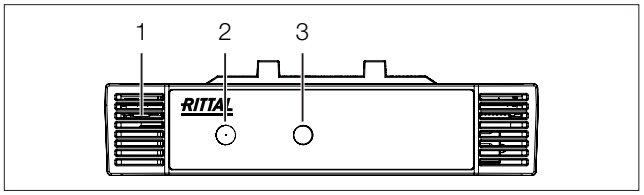


Abb. 13: Frontseite des Access Control

Legende
1 Multi-LED zur Statusanzeige
2 Infrarot-Diode (Sender)
3 Infrarot-Empfänger

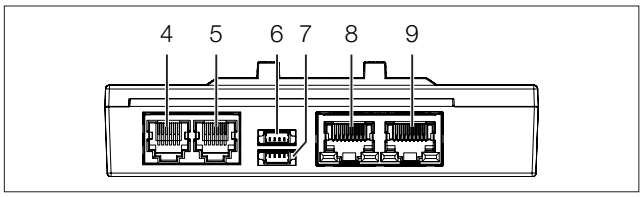


Abb. 14: Rückseite des Access Control

Legende
4 Anschluss für Griff RJ 12
5 Anschluss für Griff RJ 12
6 Anschluss für CMC III Lesegerät
7 Anschluss für CMC III Lesegerät
8 CAN-Bus-Anschluss, 24 V ⎓, 1 A
9 CAN-Bus-Anschluss, 24 V ⎓, 1 A

6.3 Anzeigen der LEDs

In der Front des Access Control ist eine Multi-LED zur Statusanzeige integriert (Abb. 13, Pos. 1). Des Weiteren sind auf der Rückseite am CAN-Bus-Anschluss (Abb. 14, Pos. 8 und 9) weitere LEDs angeordnet.

6.3.1 Anzeigen der Multi-LED

An der Multi-LED kann der Status des Access Control abgelesen werden.

Dauerlicht

Farbe	Status
Rot	Ungültiger Messwert.
Blau	Ein Software-Update des Access Control wird durchgeführt.

Tab. 2: Dauerlicht der Multi-LED

Blinkcodes

Farbe	Status
Grün	Bei Messwertänderung oder spätestens alle 5 Sekunden.
Rot	Der Zugangssensor (Access) hat den Status „Open“ oder der Vandalismus-Sensor (gValues) hat den Status „Alarm“.
Blau	Kommunikation über den CAN-Bus.

Tab. 3: Blinkcodes der Multi-LED

6.3.2 Anzeigen der LEDs am CAN-Bus-Anschluss

Am CAN-Bus-Anschluss befinden sich eine rote und eine grüne LED. Hier wird der Status des CAN-Bus angezeigt.

Farbe	Status
Grün (Dauerlicht)	Kommunikation über den CAN-Bus möglich.
Rot (Blinkend)	Übertragungsfehler.

Tab. 4: LEDs CAN-Bus-Anschluss

6.4 Bedienung über die Website des Rittal Embedded Device

Nach der Anmeldung am Rittal Embedded Device wird die Web-Oberfläche zur Bedienung des Geräts angezeigt.

- Wählen Sie zunächst im Navigationsbereich den Eintrag „CMCX-ACCC“ an.

Auf der Registerkarte **Configuration** werden analog zum Rittal Embedded Device die Zugriffsrechte für den Access Control (Schaltfläche **Device Rights**) sowie die Alarmbenachrichtigung individuell festgelegt (Schaltfläche **Alarm Configuration**).

Auf der Registerkarte **Monitoring** werden alle Einstellungen für den Access Control vorgenommen.

6.5 Verwaltung der Zugangsberechtigungen

6.5.1 Festlegen der Zugangsberechtigungen

Die Zugangsberechtigungen für die zu überwachende Tür werden auf der Registerkarte **Access Configuration** definiert.

- Wählen Sie im Konfigurationsbereich die Registerkarte **Access Configuration** an.

Zum Hinzufügen einer neuen Transponderkarte:

- Halten Sie die Transponderkarte vor den Transponderleser.

Zum Hinzufügen eines neuen Zugangscodes:

- Klicken Sie unter der Liste der bereits hinterlegten Zugangscodes bzw. Transponderkarten im Gruppenrahmen **Access** auf der Registerkarte **Access Configuration** auf die Schaltfläche **Add**.
  Es erscheint der Dialog „Access Configuraton“ analog zum Konfigurieren einer Zugangsberechtigung.

Zum Konfigurieren einer Zugangsberechtigung (Transponderkarte bzw. Zugangscode):

- Markieren Sie im Gruppenrahmen **Access** die Zeile des gewünschten Eintrags, um die hierfür hinterlegten Einstellungen anzupassen.
- Klicken Sie auf die Schaltfläche **Edit**.
  Es erscheint der Dialog „Access Configuration“.

Parameter	Erläuterung
Type	Konfiguration eines Zugangs mit Transponderkarte (Eintrag „Card“) bzw. Zahlencode (Eintrag „Keycode“).
Code	Nummer der Transponderkarte bzw. Zahlencode zum Zugang.
User	Auswahl des zum Zugang berechtigten Benutzers. Der Benutzer muss zuvor entsprechend angelegt worden sein.
Information	Indviduelle Zusatzinformation zum Zugang. Dieser Text wird zusätzlich zum User im Logfile des Rittal Embedded Device eingetragen.

Tab. 5: Gruppenrahmen Parameters

Alle angeschlossenen Griffe werden im Gruppenrahmen **Tree** angezeigt. Hier erfolgt nun die Zuordnung, welche Griffe prinzipiell mit der Zugangsberechtigung geschaltet werden können.

- Aktivieren Sie in der Baumdarstellung ggf. eine übergeordnete Gruppe (z. B. ein gesamtes „Access Control“, um alle zugewiesenen Griffe mit der Zugangsberechtigung öffnen zu können.
- Deaktivieren Sie ggf. einzelne Griffe einer Gruppe durch erneutes Anklicken.

Hinweis:
Dem Zugangscode bzw. der Transponderkarte muss ein User zugewiesen werden. Ansonsten ist der Zugang auch bei Eingabe des korrekten Zugangscodes bzw. mit der entsprechenden Transponderkarte nicht möglich.

Zum Löschen einer Zugangsberechtigung (Transponderkarte bzw. Zugangscode):

- Markieren Sie die Zeile des gewünschten Eintrags, den Sie löschen möchten.
- Markieren Sie ggf. mit gedrückter „Umschalt“-Taste einen weiteren Eintrag.
  Alle Zeilen vom zuerst gewählten Eintrag bis einschließlich dem zuletzt gewählten Eintrag werden ausgewählt.
- Markieren Sie ggf. mit gedrückter „Strg“-Taste weitere Einträge.
  Diese Zeilen werden einzeln zur Auswahl hinzugefügt.
- Klicken Sie auf die Schaltfläche **Delete**.
  Alle ausgewählten Zugangsberechtigungen werden ohne Sicherheitsabfrage direkt gelöscht.

Hinweis:
Wird eine Transponderkarte nach dem Löschen der Zugangsberechtigung wieder vor den Transponderleser gehalten, so wird wie beim Hinzufügen einer neuen Transponderkarte am Ende der Tabelle eine entsprechende Zeile angefügt.

6.5.2 Filterfunktionen

Mit Hilfe der Einstellungen im Bereich **Filter** können Sie die Liste der angezeigten Zugangsberechtigungen einschränken, z. B. nur für einen bestimmten Benutzer. Folgende Einstellungen sind hier möglich:

Parameter	Erläuterung
Type	Art der Zugangsberechtigung (Transponderkarte oder Zahlencode).
Code	Nummer der Transponderkarte bzw. Zahlencode zum Zugang.
User	Auswahl des zum Zugang berechtigten Benutzers.

Tab. 6: Filterfunktionen

Anhand eines Eintrags in in einem Feld erkennen Sie, dass ein Filter aktiv ist. Zusätzlich wird ein „Backspace“-Pfeil im jeweiligen Listenfeld angezeigt.

- Klicken Sie auf den „Backspace“-Pfeil bzw. löschen Sie den Eintrag im Feld manuell, um einen aktiven Filter aufzuheben.

6.5.3 Optionen

Im Bereich **Options** können Sie zwei Sicherheitsfunktionen aktivieren bzw. deaktivieren und das zugehörige Zeitintervall festlegen.

Vier-Augen-Modus

Bei Aktivierung des Vier-Augen-Modus müssen sich zum Öffnen eines Griffes bzw. einer Tür jeweils zwei Personen identifizieren. Hierzu müssen sich innerhalb eines einstellbaren Zeitintervalls am gleichen Kartenleser zwei verschiedene Personen mit ihren Transponderkarten bzw. ihrem Zahlencode anmelden.

Zum Aktivieren des Vier-Augen-Modus:

- Weisen Sie einer Transponderkarte bzw. einem Zahlencode im Dialog „Access Configurations“ den User „AccessAck“ zu.

DE

Dieser User ist standardmäßig auf jedem Rittal Embedded Device vorhanden und gehört zur Gruppe „Access“, der keine weitergehenden Rechte zugewiesen sind.

- Sollten der User „AccessAck“ und/oder die Gruppe „Access“ nicht vorhanden sein (z. B. weil vor einem Update des Rittal Embedded Device bereits alle Speicherplätze belegt waren), so müssen Sie den User und die Gruppe manuell anlegen (vgl. Montage-, Installations- und Bedienungsanleitung des Rittal Embedded Device).
- Stellen Sie im zugehörigen Feld „Timeout“ das Zeitintervall ein, innerhalb dessen sich die beiden Benutzer bei aktiviertem Vier-Augen-Modus anmelden müssen.

Nach dem Speichern dieser Zuordnung gilt der Vier-Augen-Modus für die **gesamte** Zugangssteuerung. Das heißt, für **jedes** Lesegerät werden mindestens zwei Transponderkarten bzw. zwei Zugangscodes benötigt.

Zum Öffnen eines Griffes bzw. einer Tür:

- Der erste Benutzer meldet sich mit seiner Transponderkarte bzw. seinem Zahlencode am Lesegerät an.
- Der zweite Benutzer meldet sich mit seiner Transponderkarte bzw. seinem Zahlencode innerhalb des eingestellten Zeitintervalls am gleichen Lesegerät an.

Wenigstens einer der beiden Benutzer muss der Benutzer „AccessAck“ sein. Die Reihenfolge, in der sich die Benutzer anmelden, ist hierbei unerheblich.

Hinweis:
Das Zeitintervall, innerhalb dessen sich die beiden Benutzer anmelden müssen, kann auch direkt in der Datei „access.cmc3“ festgelegt werden (vgl. Abschnitt 6.7 „Manuelles Anpassen der Datei „access.cmc3““).

Hinweis:
Wird zusätzlich die 2-Faktor-Authentifizierung aktiviert, wird die Funktionalität des Vier-Augen-Modus automatisch deaktiviert. Wenn einem Griff (weiterhin) der User „AccessAck“ zugewiesen ist, wird die zugehörige Checkbox „4 Eyes (Enabled)“ dennoch als „aktiv“ angezeigt.

2-Faktor-Authentifzierung

Bei Aktivierung der 2-Faktor-Authentifizierung müssen zum Öffnen eines Griffes bzw. einer Tür jeweils zwei unterschiedliche Zugangsberechtigungen eingegeben werden. Hierzu muss innerhalb eines einstellbaren Zeitintervalls sowohl eine Transponderkarte vor ein Lesegerät gehalten als auch ein Zahlencode an einem Zahlencodeschloss eingegeben werden.

Zum Aktivieren der 2-Faktor-Authentifizierung:

- Aktivieren Sie den Eintrag „2 Factor-Authentication“.
- Stellen Sie im zugehörigen Feld „Timeout“ das Zeitintervall ein, innerhalb dessen die beiden Zugangsberechtigungen eingegeben werden müssen.

Nach dem Aktivieren der 2-Faktor-Authentifizierung gilt diese für die gesamte Zugangssteuerung. Das heißt, für jeden Zugang wird sowohl eine Transponderkarte als auch ein Zugangscode benötigt.

Zum Öffnen eines Griffes bzw. einer Tür:

- Der Benutzer meldet sich mit der ersten Authentifizierung, also einer Transponderkarte bzw. einem Zahlencode, am zugehörigen Lesegerät an.
- Im Anschluss meldet sich der Benutzer mit seiner zweiten Authentifizierung innerhalb des eingestellten Zeitintervalls am zweiten zugewiesenen Lesegerät an.

Hinweis:
Das Zeitintervall, innerhalb dessen sich der Benutzer mit den beiden Zugangsberechtigungen anmelden muss, kann auch direkt in der Datei „access.cmc3“ festgelegt werden (vgl. Abschnitt 6.7 „Manuelles Anpassen der Datei „access.cmc3““).

6.5.4 Zuordnung von Lesegeräten zu Zugangsmodulen

Standardmäßig werden bei Eingabe eines berechtigten Codes bzw. Vorhalten einer berechtigten Karte an einem Lesegerät **alle** Griffe geöffnet bzw. virtuellen Access Controller geschaltet, die der jeweiligen Zugangsberechtigung im Gruppenrahmen **Tree** zugeordnet sind (vgl. Abschnitt 6.5.1 „Festlegen der Zugangsberechtigungen“).

Im Gruppenrahmen **Keypad Mapping** können nun Lesegeräte und Zugangsmodule einander zugeordnet werden. Man kann so steuern, welche Griffe bzw. Türen je nach verwendetem Lesegerät geöffnet werden.

– **Keine Zuordnung hinterlegt:** Es werden alle Zugangsmodule freigegeben, die der jeweiligen Zugangsberechtigung im Gruppenrahmen **Tree** zugeordnet sind.
– **Zuordnung zwischen Lesegerät und Zugangsmodul(en) hinterlegt:** Es werden nur die Zugangsmodule freigegeben, die hier dem jeweiligen Lesegerät zugeordnet sind. Diese Zugangsmodule müssen ebenfalls im Gruppenrahmen **Tree** der jeweiligen Zugangsberechtigung als Device zugeordnet werden.

Zum Konfigurieren der Zuordnung eines Lesegeräts zu bestimmten Griffen bzw. Türen:

- Markieren Sie im Gruppenrahmen **Keypad Mapping** die Zeile mit dem Zugangsmodul, an dem das Lesegerät angeschlossen ist, dem Sie bestimmte Griffe bzw. Türen zuordnen möchten.
- Klicken Sie auf die Schaltfläche **Edit**.
  Es erscheint der Dialog „Access Configuration“.
- Aktivieren Sie in der Baumdarstellung ggf. eine übergeordnete Gruppe (z. B. einen gesamten „Access Control“, um alle zugewiesenen Griffe am Lesegerät öffnen zu können.
- Deaktivieren Sie ggf. einzelne Griffe einer Gruppe durch erneutes Anklicken.

Hinweis:
Wird ein Lesegerät nicht einem oder mehreren Griffen zugeordnet, ist es automatisch **allen** vorhandenen Griffen zugeordnet. In diesem Fall werden also bei Verwendung dieses Lesegeräts alle Griffe bzw. Türen geöffnet, die für die Transponderkarte bzw. den Zahlencode aktiviert sind.

6.6 Registerkarte Monitoring

Auf der Registerkarte **Monitoring** werden alle Einstellungen für den Access Control vorgenommen, wie z. B. die Sensitivität des integrierten Zugangssensors.
In den folgenden Abschnitten 6.6.1 „Device“ bis 6.6.6 „Keypads > Keypad1 bzw. Keypad2“ werden jeweils nur die Parameter beschrieben, für die Sie Änderungen vornehmen können. Darüber hinaus gibt es noch Anzeigewerte, die zur Information dienen.

6.6.1 Device

Auf der Ebene „Device“ werden generelle Einstellungen zum Access Control durchgeführt.

Parameter	Erläuterung
Description	Individuelle Beschreibung des Access Control.
Location	Aufstellungsort des Access Control.

Tab. 7: Einstellungen in der Ebene „Device“

Des Weiteren werden noch Parameter angezeigt, die Detailinformationen zum Access Control liefern, wie z. B. die Version der Soft- und Hardware des Access Control. Diese Informationen sollten Sie insbesondere bei Rückfragen an Rittal bereithalten, um eine schnelle Fehlerdiagnose zu ermöglichen.

6.6.2 Access

Auf der Ebene „Access“ werden Einstellungen zum Zugangssensor durchgeführt.

Parameter	Erläuterung
DescName	Individuelle Beschreibung des Zugangssensors.
Command	Kann in Tasks verwendet werden, um den Türstatus „offen/geschlossen“ mit einem externen Sensor anstatt dem integrierten Infrarot-Sensor zu überwachen. Hierzu muss für den Parameter „Sensitivity“ der Wert „0“ eingegeben werden.
Sensitivity	Abstand Sensor zur Tür (1= klein, 3 = groß) bzw. Sensor deaktiviert (0).
Delay	Zeitliche Verzögerung, mit der die Statusmeldung geändert wird.

Tab. 8: Einstellungen in der Ebene „Access“

Hinweis:
Der Parameter „Command“ wird automatisch auf den Standardwert „Open“ gesetzt, wenn ein neuer Sensor am Bus angemeldet oder das Rittal Embedded Device neu gestartet wird.

Des Weiteren werden für den Zugangssensor noch folgende Parameter angezeigt:

Parameter	Erläuterung
Value	Aktueller Wert des Zugangssensors (0 = Tür geschlossen, 1 = Tür geöffnet).
Status	Aktueller Status des Zugangssensors unter Berücksichtigung des Delay-Wertes.

Tab. 9: Anzeigen in der Ebene „Access“

6.6.3 gValues

Auf der Ebene „gValues“ werden Einstellungen zum Vandalismussensor durchgeführt.

Parameter	Erläuterung
DescName	Individuelle Beschreibung des Vandalismussensors.
SetPtHigh-Alarm	Obere Genzbeschleunigung, bei deren Überschreiten eine Alarmmeldung ausgegeben wird.

Tab. 10: Einstellungen in der Ebene „gValues“

Des Weiteren werden für den Vandalismussensor noch folgende Parameter angezeigt:

Parameter	Erläuterung
X Axis - Value	Aktuell gemessener Beschleunigungswert in X-Richtung.
Y Axis - Value	Aktuell gemessener Beschleunigungswert in Y-Richtung.
Z Axis - Value	Aktuell gemessener Beschleunigungswert in Z-Richtung.
Status	Aktueller Status des Vandalismussensors unter Berücksichtigung des Delay-Wertes.

Tab. 11: Anzeigen in der Ebene „gValues“

Hinweis:
Wird für alle Grenzwerte auf der Ebene „gValues “ der Wert „0“ eingetragen, ist der Status des Vandalismussensors immer „OK“.

6.6.4 Handles > Handle1 bzw. Handle2 > Handle

Auf den Ebenen „Handle“ werden Einstellungen zum jeweiligen Griff durchgeführt.

DE

Parameter	Erläuterung
DescName	Individuelle Beschreibung des verwendeten Griffs.
Command	Durch Auswahl des Eintrags „Unlock“ kann ein elektromagnetischer Griff über die Website des Rittal Embedded Device entriegelt werden (Status „Unlocked“), so dass er geöffnet werden kann. Entsprechend kann ein Griff durch Auswahl des Eintrags „Lock“ verriegelt werden (Status „Locked“), so dass er nicht geöffnet werden kann. Durch Auswahl des Eintrags „Delay“ wird der Griff für die im Feld „Delay“ angegebene Zeit entriegelt und im Anschluss wieder verriegelt.
Delay	Zeitliche Verzögerung, mit der die Statusmeldung geändert wird.

Tab. 12: Einstellungen in der Ebene „Handle“

Des Weiteren werden für den jeweiligen Griff noch folgende Parameter angezeigt:

Parameter	Erläuterung
Value	Aktueller Zustand des verwendeten Griffs (0 = Griff geschlossen, 1 = Griff geöffnet).
Status	Aktueller Status der Verriegelung.

Tab. 13: Anzeigen in der Ebene „Handle“

Hinweis:
Die o. g. beschriebene Logik des Werts „Value“ gilt für die Griffe DK 7030.610 und DK 7030.611. Bei anderen Griffsystemen kann die Logik umgekehrt sein (0 = Griff geöffnet, 1 = Griff geschlossen).

Hinweis:
Wird der Griff vom Access Control getrennt, wird keine Fehlermeldung ausgegeben. Der Status des Griffs ändert sich auf „Inactive“ und es wird eine entsprechende Meldung in den Log-Informationen erzeugt. Diese Status-Änderung kann in einem Task abgefragt und mit einer Aktion verknüpft werden.

Hinweis:
Wird der Griff mit dem Masterkey geöffnet, zeigt das Rittal Embedded Device eine Alarmmeldung an. Diese kann durch Schließen des Griffs wieder beseitigt werden.

6.6.5 Handles > Handle1 bzw. Handle2 > LED

Auf der Ebene „LED“ werden Einstellungen zur LED-Anzeige im jeweiligen Griff durchgeführt.

Parameter	Erläuterung
Mode	Steuerung der LED-Anzeige im Griff „Off“: LED-Anzeige dauerhaft ausgeschaltet. „Access“: Anzeige entsprechend dem Schaltzustand des Griffs bzw. des Status des Access Control. „Access & beeper“: Analog wie „Zugang“, zusätzlich ertönt im Fehlerfall ein Signalton. „CMC“: Anzeige entsprechend dem Zustand des Rittal Embedded Device. „CMC & beeper“: Analog wie „CMC“, zusätzlich ertönt im Fehlerfall ein Signalton. „Task“: Anzeige entsprechend der Auswertung eines Tasks (Variable „LED. Command“). „Task & beeper“: Analog wie „Task“, zusätzlich ertönt im Fehlerfall ein Signalton.
Command	Bei Auswahl des Modes „Task“ kann hier die Farbe der LED eingestellt werden. Die Farbe wird bis zum nächsten Auslösen des Tasks beibehalten. Wird hier „Custom“ ausgewählt, kann die Farbe über die drei Komponenten rot, grün und blau definiert werden.
Red	Rotanteil der Farbe
Green	Grünanteil der Farbe
Blue	Blauanteil der Farbe

Tab. 14: Einstellungen in der Ebene „LED“

6.6.6 Keypads > Keypad1 bzw. Keypad2

Auf der Ebene „KeyPad“ werden Einstellungen zum jeweiligen Zahlencodeschloss bzw. zum jeweiligen Transponderleser durchgeführt.

Parameter	Erläuterung
DescName	Individuelle Beschreibung des verwendeten Zahlencodeschlosses bzw. Transponderlesers
Command	Durch Auswahl des Eintrags „On“ wird das angeschlossene Zahlencodeschloss bzw. der angeschlossene Transponderleser aktiviert. Entsprechend kann ein angeschlossenes Lesegerät durch Auswahl des Eintrags „Off“ deaktiviert werden, so dass es **nicht** zum Öffnen der Tür verwendet werden kann.

Tab. 15: Einstellungen in der Ebene „Keypad“

Des Weiteren werden für das jeweilige Zahlencodeschloss bzw. den jeweiligen Transponderleser noch folgende Parameter angezeigt:

Parameter	Erläuterung
Status	Zeigt an, ob ein Zahlencodeschloss bzw. ein Transponderleser angeschlossen wurde (active) oder nicht (inactive) bzw. das Lesegerät deaktiviert wurde (off).

Tab. 16: Anzeigen in der Ebene „Keypad“

6.7 Manuelles Anpassen der Datei „access.cmc3“

Die Einstellungen zu den Zugangsberechtigungen können alternativ auch direkt in der Datei „access.cmc3“ vorgenommen werden. Diese Datei wird beim ersten Starten des Rittal Embedded Device automatisch im Verzeichnis „upload“ des Rittal Embedded Device angelegt.

Hinweis:
Wird die Datei „access.cmc3“ aus dem Ordner entfernt, ist ein Zugang nur noch mit den drei standardmäßig freigegebenen Zugangscodes „1001“, „1002“ und „1003“ möglich. Alle anderen Zugangsberechtigungen müssen zunächst wieder in einer neu angelegten Datei hinterlegt werden.

6.7.1 Download der Datei

Hinweis:
Die folgenden Beschreibungen gehen davon aus, dass Sie die (S)FTP-Verbindung mit dem Programm „FileZilla“ herstellen. Bei Verwendung eines anderen Programms müssen Download und Upload der Datei evtl. anders durchgeführt werden.

- Stellen Sie von einem PC aus zunächst eine FTP- oder SFTP-Verbindung zum Rittal Embedded Device her (vgl. Montage-, Installations- und Bedienungsanleitung zum Rittal Embedded Device).
- Wechseln Sie im linken Teilfenster (PC) in den Ordner, in dem Sie die Datei „access.cmc3“ lokal speichern möchten.
- Wechseln Sie im rechten Teilfenster (Rittal Embedded Device) in den Ordner „upload“.
- Klicken Sie mit der rechten Maustaste auf die Datei „access.cmc3“ und wählen Sie die Aktion „Download“ aus.
- Trennen Sie die (S)FTP-Verbindung zwischen dem PC und dem Rittal Embedded Device.

Sollte im Verzeichnis „upload“ keine Datei „access.cmc3“ vorhanden sein, so muss diese zunächst angelegt werden.

- Bei Verwendung eines Zahlencodeschlosses: Geben Sie am Zahlencodeschloss eine beliebige Zahlenfolge ein und bestätigen Sie diese mit der „Enter“-Taste. Die Datei wird nun im Ordner „upload“ erzeugt.
- Bei Verwendung eines Transponderlesers: Halten Sie eine beliebige Transponderkarte vor das Lesegerät. Die Datei wird nun im Ordner „upload“ erzeugt.
- Stellen Sie erneut eine (S)FTP-Verbindung zwischen dem PC und dem Rittal Embedded Device her und laden Sie die Datei herunter.
- Trennen Sie wiederum die (S)FTP-Verbindung zwischen dem PC und dem Rittal Embedded Device.

6.7.2 Bearbeiten der Datei

Die Datei kann nun mit einem Text-Editor bearbeitet werden. Rittal empfiehlt, hierzu statt des standardmäßig unter Windows installierten „Notepad“ das Programm „Notepad++“ zu verwenden. Dieses ist als Freeware im Internet verfügbar.

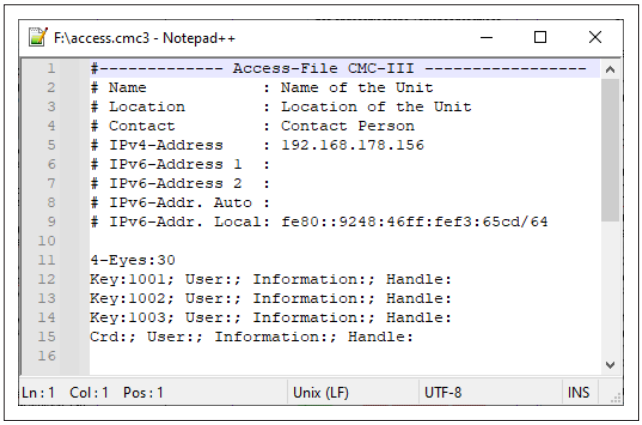


Abb. 15: Datei „access.cmc3“ in Notepad++

Die Datei besitzt folgenden Aufbau:

– Zeilen mit einem „#“ an erster Stelle sind Kommentarzeilen. Hier sind grundlegende Informationen zum Rittal Embedded Device hinterlegt.
– Zeilen mit „Key“ bzw. „Crd“ als erstem Eintrag enthalten bei Verwendung eines Zahlencodeschlosses die freigegebenen Zugangscodes sowie bei Verwendung eines Transponderlesers die freigegebenen Kartennummern der Transponderkarten (vgl. Abschnitt 6.5.1 „Festlegen der Zugangsberechtigungen“).
– Die Zeile mit „4-Eyes“ als erstem Eintrag enthält das Zeitintervall für die Anmeldung im Vier-Augen-Modus (vgl. Abschnitt 6.5.3 „Optionen“).
– Zeilen mit „Keypad“ als erstem Eintrag enthalten die Zuordnung von Lesegeräten zu einzelnen Zugangsmodulen (vgl. Abschnitt 6.5.4 „Zuordnung von Lesegeräten zu Zugangsmodulen“).

Zugangscodes bzw. Transponderkarten

Die Zeilen für die Zugangscodes bzw. die Transponderkarten enthalten folgende Einträge:

Parameter	Erläuterung
Key	Zugangscode mit bis zu acht Stellen für ein Zahlencodeschloss, der zum Zugang berechtigt.

DE

Parameter	Erläuterung
Crd	Kartennummer einer Transponderkarte, die zum Zugang berechtigt.
User	Benutzer, der beim Öffnen des Zahlencodeschlosses mit dem zugehörigen Zahlencode bzw. beim Öffnen mit der zugehörigen Transponderkarte im Logfile des Rittal Embedded Device eingetragen wird. Dieser Benutzer muss im Rittal Embedded Device vorhanden sein.
Information	Individuelle Zusatzinformation zum Zugang. Dieser Text wird zusätzlich zum User im Logfile des Rittal Embedded Device eingetragen.
Handle	Seriennummer des Access Control bzw. des (virtuellen) Access Controllers, an dem das zu schaltende Zugangsmodul angeschlossen ist. Hier können auch mehrere, durch Komma getrennte Einträge für unterschiedliche Access Control hinterlegt werden.

Tab. 17: Einträge für Zugangscodes bzw. Transponderkarten

Hinweis:
In jeder Zeile befindet sich entweder der Parameter „Key“ oder der Parameter „Crd“, je nachdem ob die Zeile für das Zahlencodeschloss oder den Transponderleser gilt.

Anhand der folgenden Beispielkonfiguration werden die Einträge im Detail erläutert.

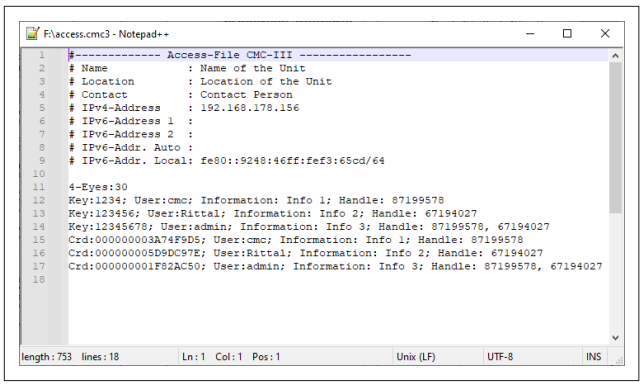


Abb. 16: Beispielkonfiguration

Die Datei besitzt folgenden Aufbau:

– Mit dem Zugangscode „1234“ wird ein erster Griff geöffnet (Zeile 11 im Editorfenster). Der Benutzer „cmc“ und die Information „Info 1“ werden im Logfile des Rittal Embedded Device eingetragen.
– Mit dem Zugangscode „123456“ wird ein zweiter Griff geöffnet (Zeile 12). Der Benutzer „Rittal“ und die Information „Info 2“ werden im Logfile des Rittal Embedded Device eingetragen.
– Mit dem Zugangscode „12345678“ werden beide Griffe geöffnet (Zeile 13). Der Benutzer „admin“ und die Information „Info 3“ werden im Logfile des Rittal Embedded Device eingetragen.

In den Zeilen 15 bis 17 ist den Benutzern zusätzlich je eine Transponderkarte zugeordnet. Diese Transponderkarten öffnen die gleichen Griffe wie die o. g. Zugangscodes. Es werden die jeweils angegebenen Benutzer sowie die zugehörigen Informationen im Logfile des Rittal Embedded Device eingetragen.

Zeitintervall für den Vier-Augen-Modus

In der Zeile mit dem Eintrag „4-Eyes“ wird das Zeitintervall für die Anmeldung im Vier-Augen-Modus festgelegt.

Parameter	Erläuterung
4-Eyes	Zeitintervall in Sekunden, innerhalb dessen sich die beiden Personen mit ihren Transponderkarten bzw. ihrem Zahlencode anmelden müssen.

Tab. 18: Zeitintervall für den Vier-Augen-Modus

Zuordnung von Lesegeräten zu Zugangsmodulen

Die Zeilen für die Zuordnung von Lesegeräten zu Zugangsmodulen enthalten folgende Einträge:

Parameter	Erläuterung
Keypad	Seriennummer des Access Control bzw. des (virtuellen) Access Controllers, an dem das zu Lesegerät angeschlossen ist, dem die folgenden Griffe bzw. Türen zugeordnet werden.
Handle	Seriennummer des Access Control bzw. des (virtuellen) Access Controllers, an dem das zu schaltende Zugangsmodul angeschlossen ist. Hier können auch mehrere, durch Komma getrennte Einträge für unterschiedliche Access Control hinterlegt werden.

Tab. 19: Zuordnung von Lesegeräten zu Zugangsmodulen

Hinweis:
Ist dem Eintrag „Handle“ **kein** Zugangsmodul zugeordnet, wird das Lesegerät **allen** Zugangsmodulen zugeordnet. In diesem Fall werden also alle Türen geöffnet, die für die Transponderkarte bzw. den Zahlencode aktiviert sind, unabhängig davon, welches Lesegerät genutzt wird.

6.7.3 Hochladen der Datei

Nachdem alle Einträge in die Datei „access.cmc3“ erfolgt sind, muss diese Datei wieder auf dem Rittal Embedded Device im Verzeichnis „upload“ abgelegt werden.

■ Stellen Sie von einem PC aus wiederum eine FTP- oder SFTP-Verbindung zum Rittal Embedded Device her.

- Wechseln Sie im rechten Teilfenster (Rittal Embedded Device) in den Ordner „upload“.
- Wechseln Sie im linken Teilfenster (PC) in den Ordner, in dem Sie die überarbeitete Version der Datei „access.cmc3“ abgelegt haben.
- Klicken Sie mit der rechten Maustaste auf die Datei „access.cmc3“ und wählen Sie die Aktion „Hochladen“ aus.
- Falls das Hochladen der Datei so nicht möglich ist, löschen Sie zunächst die vorhandene Datei „access.cmc3“ aus dem Verzeichnis „upload“ heraus und laden Sie die Datei vom PC dann erneut hoch.
- Trennen Sie die abschließend (S)FTP-Verbindung zwischen dem PC und dem Rittal Embedded Device.

Die Zugangsberechtigungen sind nun aktualisiert.

DE

7 Lagerung und Entsorgung

7.1 Lagerung

Wenn das Gerät über einen längeren Zeitraum nicht im Einsatz ist, empfiehlt Rittal das Gerät spannungsfrei zu schalten und vor Feuchtigkeit und Staub zu schützen.

7.2 Entsorgung

Da der Access Control hauptsächlich aus den Bestandteilen „Gehäuse“ und „Leiterplatte“ besteht, ist das Gerät zur Entsorgung der Elektronikverwertung zuzuführen.

DE

8 Technische Daten

Technische Daten		DK Access Control
Best.-Nr.		7010.180
B x H x T (mm)		110 x 30 x 40
Temperatureinsatzbereich		0 °C…+55 °C
Lagertemperatur		-20 °C…+70 °C
Feuchtigkeitseinsatzbereich		5 %…95 % relative Feuchte, nicht kondensierend
Arbeitsweise		optisch
Sender		Infrarot-Diode
Empfänger		Infrarot-Empfänger
Schutzart		IP 30 nach IEC 60 529
Ein- und Ausgänge	CAN-Bus (RJ 45)	2 x
	Griff (RJ 12)	2 x
	Anschluss für CMC III Lesegerät	2 x
Bedienung/Signale	LED-Anzeige	OK/Warnung/Alarm/Status CAN-Bus

Tab. 20: Technische Daten

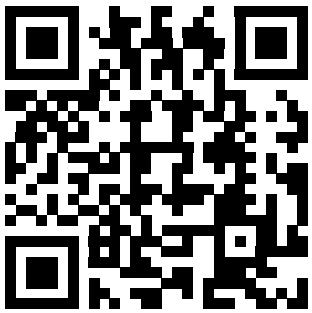
DE

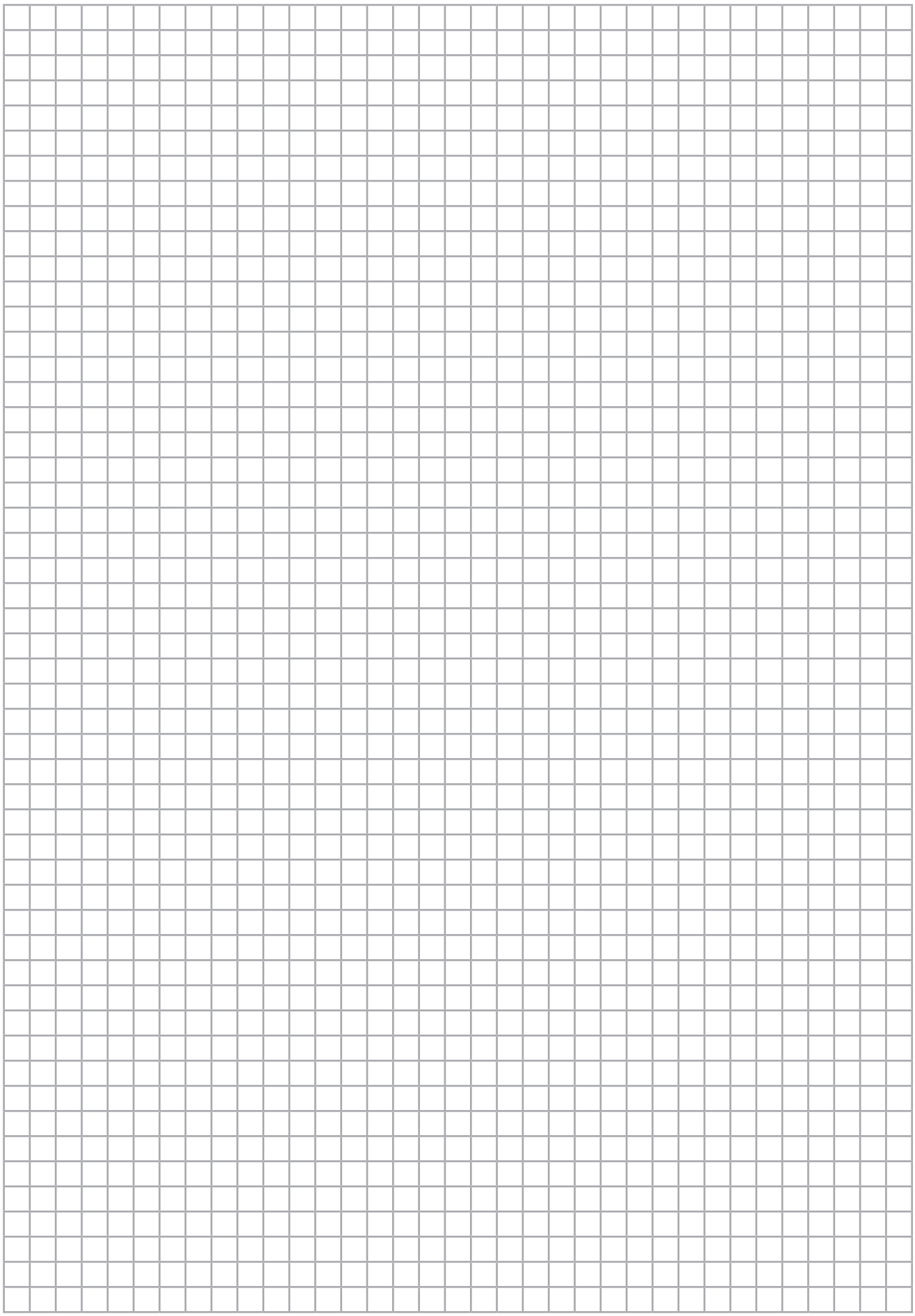
9 Kundendienstadressen

Zu technischen Fragen wenden Sie sich bitte an:
Tel.: +49(0)2772 505-9052
E-Mail: info@rittal.de
Homepage: www.rittal.de

Bei Reklamationen oder Servicebedarf wenden Sie sich bitte an:
Tel.: +49(0)2772 505-1855
E-Mail: service@rittal.de

Kontaktdaten finden Sie auf der Internetseite von Rittal unter folgender Adresse:
– https://www.rittal.de/Rittal-Standorte





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

08.2025/D-0000-00004721-00

RITTAL GmbH & Co. KG
Auf dem Stuetzelberg · 35745 Herborn · Germany
Phone +49 2772 505-0
E-mail: info@rittal.de · www.rittal.com