Rittal – The System.

Faster – better – everywhere.

DK access control

7010.180

Assembly and operating instructions

ENCLOSURES | POWER DISTRIBUTION | CLIMATE CONTROL | IT INFRASTRUCTURE | SOFTWARE & SERVICES

FRIEDHELM LOH GROUP

EN

Foreword

Dear Customer,

Thank you for choosing our access control!

We wish you every success.

Yours
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.com
www.rittal.com
www.rittal.de

We are always happy to answer any technical questions regarding our entire range of products.

EN

Contents

EN

1 Notes on documentation

1.1 CE labelling

Rittal GmbH & Co. KG hereby confirms that the access control is compliant with the EU EMC Directive 2014/30/EU. An appropriate declaration of conformity has been prepared. It can be provided on request.

CE

1.2 Storing the documents

The assembly and operating instructions as well as all applicable documents are an integral part of the product. They must be passed to those persons who are engaged with the unit and must always be available and on hand for the operating and maintenance personnel.

1.3 Symbols used in these operating instructions

The following symbols are used in this documentation:

Danger!
A dangerous situation in which failure to comply with the instructions will result in death or severe injury.

Warning!
A dangerous situation which may cause death or serious injury if the instructions are not followed.

Caution!
A dangerous situation which may lead to (minor) injuries if the instructions are not followed.

Note:
Important notices and indication of situations which may result in material damage.

■ This symbol indicates an "action point" and shows that you should perform an operation or procedure.

1.4 Associated documents

– Installation and Short User Guide
– Assembly and operating instructions of the Rittal embedded device used

1.5 Area of validity

This documentation shows the English screenshots. English terminology is also used in the descriptions of the individual parameters on the Rittal embedded device website. Depending on the set language, the displays on the Rittal embedded device website may be different (see assembly and operating instructions for the Rittal embedded device used).

2 Safety instructions

2.1 General safety instructions

Please observe the subsequent general safety instructions for the installation and operation of the system:

– The access control may only be assembled and installed by properly trained specialists.
– The casing of the access control must not be opened!
– The access control must not come into contact with water, aggressive or flammable gases and vapours!
– The access control can be used only within the limits of the specified technical data!
– The access control may only be supplied with the required operating voltage via the CAN bus.
– The access control must not be used in locations where children might be present.
– Use only original Rittal products or products recommended by Rittal in conjunction with the access control.
– Please do not make any changes to the access control that are not described in this manual or in the associated manuals.
– The operational safety of the access control is guaranteed only for its approved use. The technical specifications and limit values stated must not be exceeded under any circumstances. In particular, this applies to the specified ambient temperature range and IP degree of protection.
– Other than these general safety instructions, ensure you also observe the specific safety instructions when the tasks described in the following chapters are performed.

REACH safety information in accordance with Regulation (EC) No 1907/2006

– The product contains the SVHC "Lead – CAS no. 7439-92-1".
– The manufacturer specifies that no health risks of any kind arise during use of the product when handled properly.
– After use, the product must be disposed of properly in accordance with the applicable statutory regulations.

2.2 Service and technical staff

– The mounting, installation, commissioning, maintenance and repair of this unit may only be performed by qualified mechanical and electro-technical trained personnel.
– Only properly instructed personnel may work on a unit while in operation.

EN

3 Product description

3.1 Functional description and components

3.1.1 Function

The access control is used for monitoring rack doors via an infrared access sensor as well as general vibration monitoring. A CMC III reader unit and a handle can also be connected to the interfaces. The access sensor signals whether the door is open or closed. The codes for the door release can be entered on the reader unit. An electrical handle then can be used to open the door and monitor the door handle. The access control has an identification that allows it to be detected automatically by the Rittal embedded device.

3.1.2 Components

The device consists of a compact plastic housing in RAL 9005 with a ventilated front.

3.2 Intended use, foreseeable misuse

The access control is solely intended for access and general vibration monitoring on a server rack. It must only be used in conjunction with Rittal embedded devices (software version 10.0.0 or above). Envisaged deployment locations are enclosures and enclosure systems, as well as racks for the installation of server and network technology in secure and technology rooms. The access control must only be combined and operated with the intended Rittal system accessories and cables (see Assembly and Operating Instructions for the CMC III Processing Unit – Document D-0000-00000553-00). Any other use is not permitted.

The unit is state of the art and built according to recognised safety regulations. Nevertheless, incorrect use may result in damage to or faults with the system and other material assets.

Consequently, the unit must only be used properly and in a technically sound condition! Any malfunctions which impair safety should be rectified immediately! Follow the operating instructions!

The intended use also includes the observance of the documentation provided and fulfilling the inspection and maintenance conditions.

Rittal GmbH & Co. KG is not liable for any damage which may result from failure to comply with the documentation provided. The same applies to the non-observance of the valid documentation for any deployed accessories and the Rittal embedded device.

Inappropriate use may result in danger. Inappropriate use includes:

– Use of impermissible tools.
– Improper operation.
– Improper rectification of malfunctions.
– Use of accessories not approved by Rittal GmbH & Co. KG.

3.3 Scope of supply

– Access control
– Accessories provided (fig. 1)
– Installation and Short User Guide

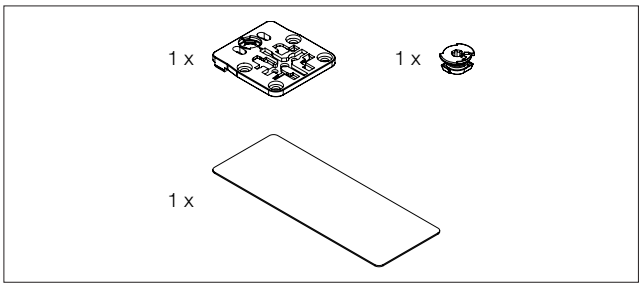

Fig. 1: Accessories provided

EN

4 Transport and handling

4.1 Transport

The unit is delivered in a carton.

4.2 Unpacking

- Remove the unit's packaging materials.

Note:
After unpacking, the packaging materials must be disposed of in an environmentally friendly way. They consist of the following materials: Polyethylene film (PE film), cardboard.

- Check the unit for any damage that may have occurred during transport.

Note:
Damage and other faults, e.g. incomplete delivery, should be reported immediately, in writing, to the shipping company and to Rittal GmbH & Co. KG.

- Remove the unit from the PE film.
- Remove the protective film from the front cover of the device.

EN

5 Installation

5.1 Safety instructions

- Please observe the valid regulations for installation in the country in which the access control is installed and operated, and the national regulations for accident prevention. Please also observe any internal company regulations, such as work, operating and safety regulations.
- The technical specifications and limit values stated must not be exceeded under any circumstances. In particular, this applies to the specified ambient temperature range and IP degree of protection.
- If a higher IP protection class is required for a special application, the access control must be installed in an appropriate housing or in an appropriate enclosure with the required IP degree of protection. Under certain circumstances, the integral infrared sensor may then no longer function.

5.2 Siting location requirements

To ensure the unit functions correctly, the conditions for the installation site of the unit specified in section 8 "Technical specifications" must be observed.

Electromagnetic interference

– Interfering electrical installations (high frequency) should be avoided.

5.3 Installation procedure

There are generally several options for installing the access control:

1. Installation on the frame of the enclosure or IT enclosure using the bracket included.
2. Installation with the provided bracket on a punched section with mounting flange.
3. Optional: Installation on a top-hat rail using the bracket included along with a spring clip (accessories).

5.3.1 Installation notes

- Install the access control in such a way that the front with the transmitter and receiver points toward the door to be monitored.
- Preferably, install the access control in such a way that the infrared access sensor points toward the lock-side and not the hinge-side of the door to be monitored.

  Because the angle of the reflecting foil changes faster, an opened door will be detected faster.
- The access control must be positioned so that it is ventilated with an adequate amount of air and the ventilation slots are not covered.
- Glue the reflecting foil provided at the door position exactly opposite the infrared access sensor.
- Ensure observance of the minimum and maximum clearances between the sensor and the reflecting foil that depend on the set value for "sensitivity" specified in the following table.

Sensitivity	**Min. clearance** mm	**Max. clearance** mm
1	20	70
2	20	100
3	20	130

Tab. 1: Minimum and maximum clearances

Note:
In the delivered state, the sensitivity is preset to the value "2".

- Ensure that the access control is installed only in one of the shown positions.

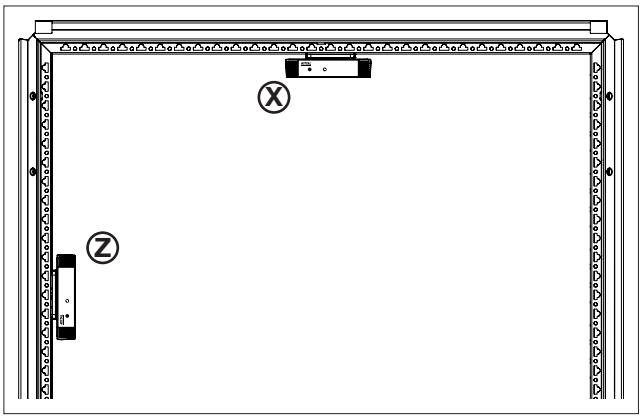

Fig. 2: Mounting positions

5.3.2 Installation with the provided bracket on the enclosure frame

The provided bracket is used for installation on the frame of an IT enclosure.

- For installation on a TS IT enclosure, break off the protruding lugs at the rear of the bracket.

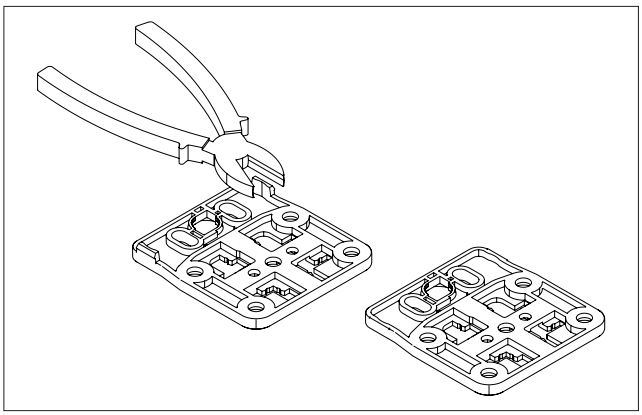

Fig. 3: Preparing the bracket for installation on a TS IT enclosure

- Place the access control on the bracket from above.

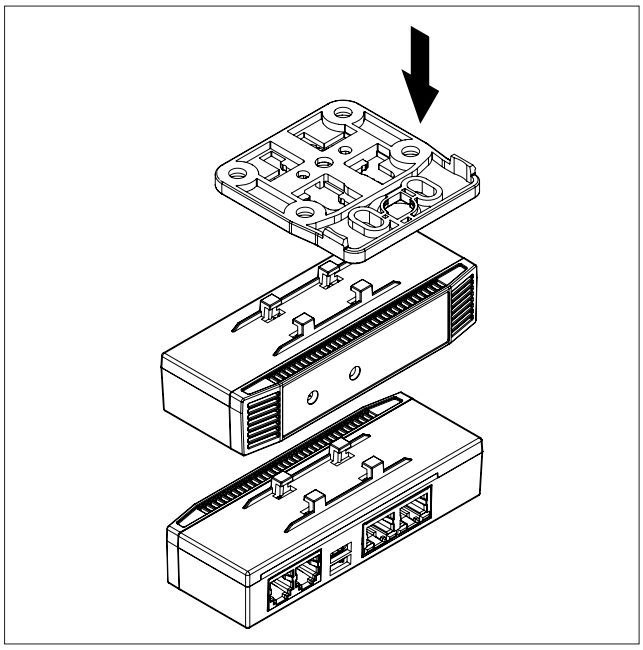

Fig. 4: Attaching the sensor to the bracket

- Move the sensor sideways slightly on the bracket so that it latches into place.

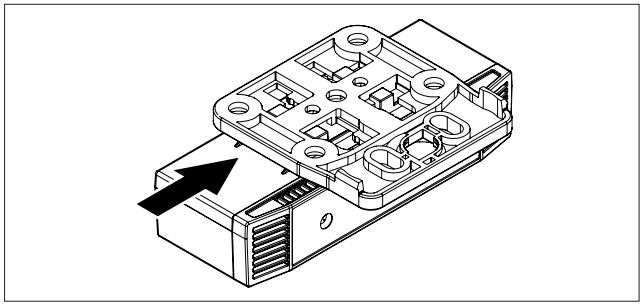

Fig. 5: Latching the sensor into place on the bracket

- Fasten the bracket, including access control, at the desired position in the enclosure or the IT enclosure by making a quarter-turn of the connector.

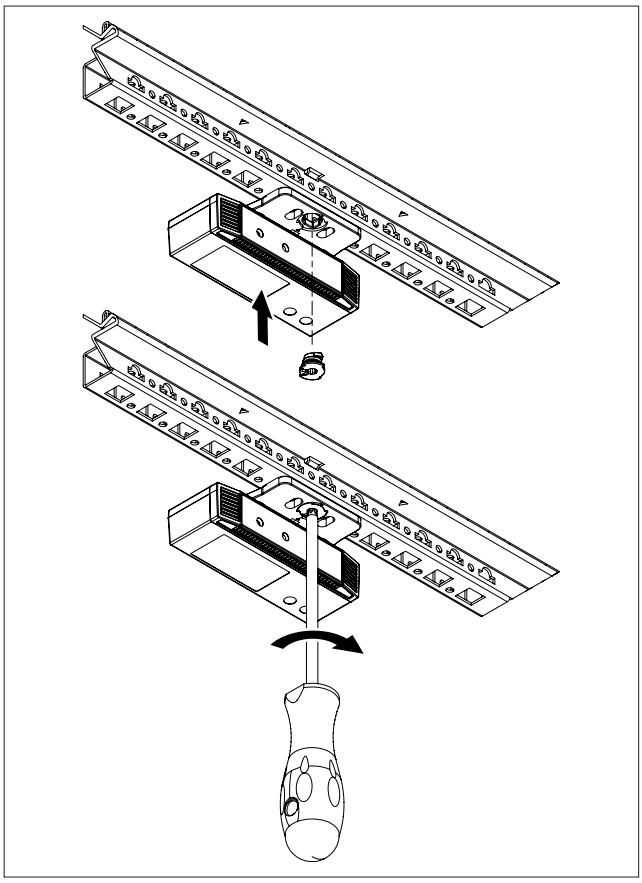

Fig. 6: Mounting the enclosure section "X"

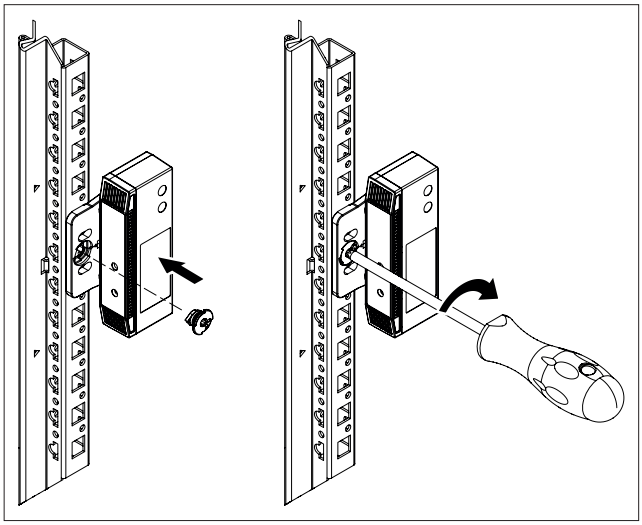

Fig. 7: Mounting the enclosure section "Z"

- Optionally secure the bracket using the two screws M5.5 x 13.

EN

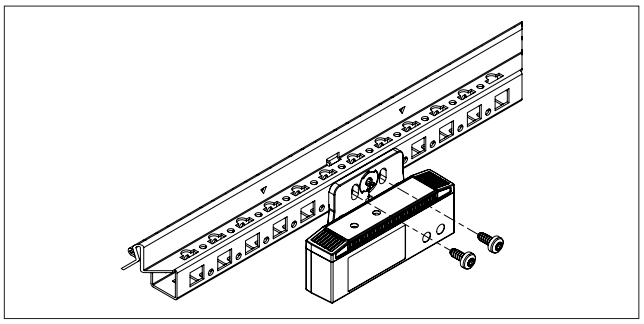

Fig. 8: Optional securing of the bracket (enclosure section "X" or enclosure section "Z")

5.3.3 Installation with the provided bracket on a punched section with mounting flange

The provided bracket is used for installation on a punched section with mounting flange.

- Place the access control on the bracket from above and latch it similar to the installation on the enclosure frame.
- Fasten the bracket, including access control, at the desired position in the enclosure on the punched section with mounting flange by making a quarter-turn of the connector.

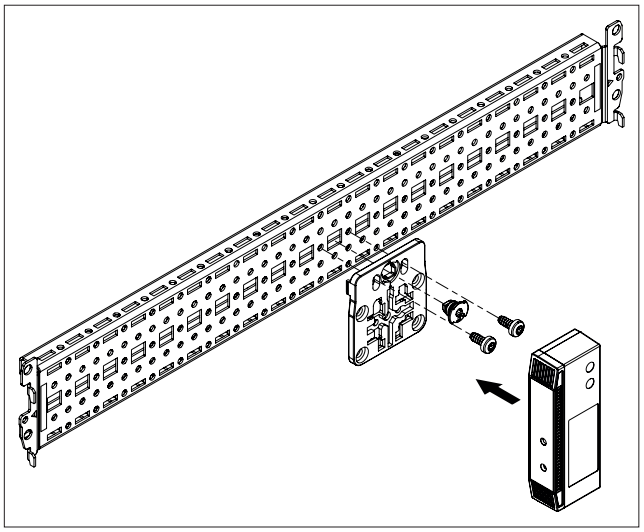

Fig. 9: Fastening the sensor to a punched section with mounting flange

- Optionally secure the bracket using the two screws M5.5 x 13 similar to the installation on the enclosure frame.

5.3.4 Installation on a top-hat rail

The sensor can also be mounted on a top-hat rail using the bracket included in the scope of delivery along with a spring clip (accessories).

- First screw the bracket onto the spring clip for installation on a top-hat rail using two screws M4 x 10.
- Then place the access control on the bracket and latch it into place.

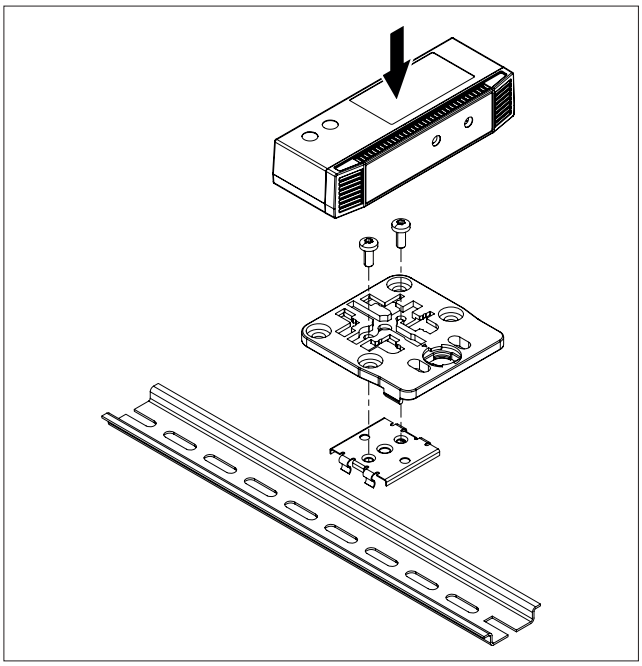

Fig. 10: Fastening the bracket to the spring clip

- Latch the spring clip into place at the desired position on the top-hat rail.

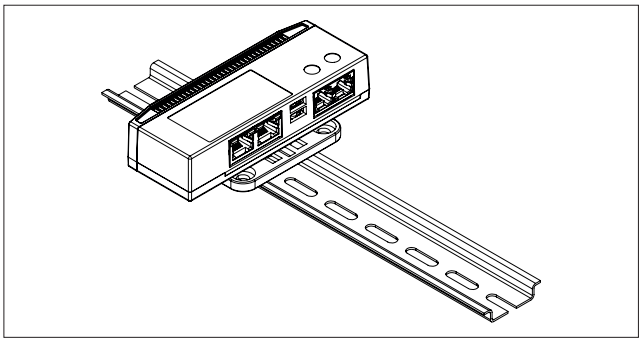

Fig. 11: Sensor with spring clip on the top-hat rail

5.4 Connection of the sensor

The access control is supplied with the necessary operating voltage via the CAN bus connection. A separate power supply unit does not need to be connected.

- If necessary, connect the following connection accessories to the appropriate connection. (fig. 12, item 4 to 7).
  - CMC III coded lock VX (7030.222, 7030.223)
  - CMC III transponder reader VX (7030.232, 7030.233)
  - CMC III online comfort handle (7030.610, 7030.611)
  - Electromagnetic Ergoform-S handle (7320.700)
  - Electromagnetic TS 8 handle with master key function with and without CCP (7320.721)
- Use a CAN bus connection cable to connect the access control to a CAN bus interface on the Rittal embedded device or the neighbouring component on the CAN bus (fig. 12, item 8, 9).

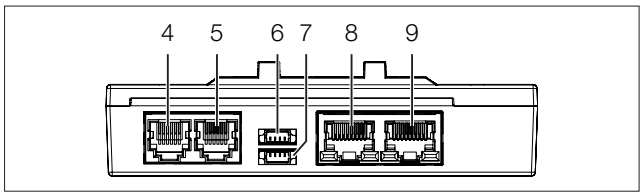

Fig. 12: Rear of the access control

Key

4 Connection for RJ 12 handle
5 Connection for RJ 12 handle
6 Connection for CMC III reader unit
7 Connection for CMC III reader unit
8 CAN bus connection, 24 V ⎓, 1 A
9 CAN bus connection, 24 V ⎓, 1 A

The following CAN bus connection cables are available from Rittal:

– DK 7030.090 (length 0.5 m)
– DK 7030.091 (length 1 m)
– DK 7030.092 (length 1.5 m)
– DK 7030.093 (length 2 m)
– DK 7030.480 (length 3 m)
– DK 7030.490 (length 4 m)
– DK 7030.094 (length 5 m)
– DK 7030.095 (length 10 m)

The sensor software is updated, if necessary, after being connected. The status LED of the access control glows blue throughout the entire update process, while the sensor itself is being updated.
In addition, the status LED of the Rittal embedded device flashes white and a corresponding message appears on the website.

Note:
No settings can be modified as long as the update process is running.

The update of the sensor is complete when the following conditions have been fulfilled:

1. The LEDs on the bus connection of the sensor light green.
2. The multi-LED of the sensor behind the front panel flashes blue and also green, yellow or red depending on the status of the sensor.

Further components are connected as a daisy chain.

- When connecting other components to the CAN bus, please note the following restrictions:
  – When installing sensors or other compatible components, the total current per CAN bus channel must not exceed 1 A.
  – Electricity consumption of access control: 40 mA plus 125 mA per connected handle
- If necessary, connect another component (e.g. another sensor type) to the second, free CAN bus interface of the access control (fig. 12, item 8, 9).

Status change display:

– The two green and the two red CAN bus LEDs on the CAN bus connection flash.
– The multi-LED of the Rittal embedded device flashes continually in the sequence green – yellow – red.
– The multi-LED of the access control flashes blue continuously.

- Press the "C" key on the Rittal embedded device (an initial audio signal will sound) and keep it pressed for approx. 3 seconds until a second audio signal is heard.

Note:
See section 6.3.1 "Multi-LED displays" for a list of all of the multi-LED displays.

EN

6 Operation

6.1 Activating the access control

After connecting the access control to a neighbouring component using a CAN bus connecting cable, the access control starts automatically (see section 5.4 "Connection of the sensor"). Separate activation is not required.

6.2 Operating and display elements

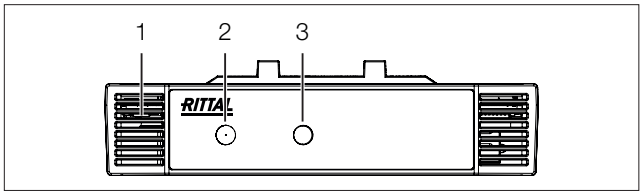

Fig. 13: Front of the access control

Key

1 Multi-LED for status display
2 Infrared diode (transmitter)
3 Infrared receiver

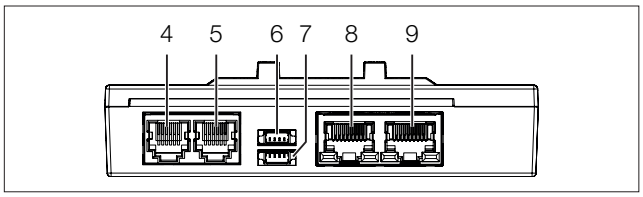

Fig. 14: Rear of the access control

Key

4 Connection for RJ 12 handle
5 Connection for RJ 12 handle
6 Connection for CMC III reader unit
7 Connection for CMC III reader unit
8 CAN bus connection, 24 V ⎓, 1 A
9 CAN bus connection, 24 V ⎓, 1 A

6.3 LED displays

A multi-LED for the status display is integrated into the front of the access control (fig. 13, item 1). Further LEDs are located at the rear on the CAN bus connection (fig. 14, item 8 and 9).

6.3.1 Multi-LED displays

The status of the access control can be read on the multi-LED.

Continuously lit

Colour	Status
Red	Invalid measured value.
Blue	An access control software update is being carried out.

Tab. 2: Multi-LED continuously lit

Flashing codes

Colour	Status
Green	When the measured value changes or, at the latest, every 5 seconds.
Red	The access sensor (Access) has the status "Open" or the vandalism sensor (gValues) has the status "Alarm".
Blue	Communication via the CAN bus.

Tab. 3: Multi-LED flashing codes

6.3.2 LED displays on the CAN bus connection

A red and a green LED are located on the CAN bus connection. They display the status of the CAN bus.

Colour	Status
Green (continuously lit)	Communication via the CAN bus possible.
Red (flashing)	Transmission fault.

Tab. 4: LEDs for the CAN bus connection

6.4 Operating from the Rittal embedded device website

After logging on to the Rittal embedded device, the web interface for operating the device is displayed.

- First select the "CMCX-ACCC" entry in the navigation area.

Similar to the Rittal embedded device, the **Configuration** tab can be used to individually configure the access rights for the access control (**Device Rights** button) and the alarm messages (**Alarm Configuration** button).

The **Monitoring** tab is used to configure all of the settings for the access control.

6.5 Management of access authorisations

6.5.1 Specification of the access authorisations

The access authorisations for the door to be monitored are defined in the **Access Configuration** tab.

- Select the **Access Configuration** tab in the configuration area.

To add a new transponder card:

- Hold the transponder card in front of the transponder reader

To add a new access code:

- Below the list of access codes / transponder cards that have already been added in the **Access** groupframe of the **Access Configuration** tab, click the **Add** button.

The "Access Configuration" dialogue appears in the same way as configuring an access authorisation.

To configure an access authorisation (transponder card or access code):

- Select in the **Access** group frame the line with the required entry to adapt the associated settings.
- Click the **Edit** button.
  The "Access Configuration" dialogue opens.

Parameter	Explanation
Type	Configuration of an access via transponder card ("Card" entry) or access code ("Keycode" entry).
Code	Number of the transponder card or access code for access.
User	Selection of the user authorised for the access. The user must have been created in advance.
Information	Specific additional information for the access. This text is also added for the user in the Rittal embedded device logfile.

Tab. 5: Parameters group frame

All connected handles are displayed in the **Tree** group frame. The handles that generally can be switched with the access authorisation are now assigned here.

- If necessary, enable a higher-level group in the tree representation (e.g. an entire "Access Control") to open all assigned handles with access authorisation.
- If necessary, disable individual handles of a group by reclicking them.

Note:
A user must be assigned to the access code or transponder card. Otherwise, access isn't possible even if the correct access code is entered or with the appropriate transponder card.

To delete an access authorisation (transponder card or access code):

- Select the line with the required entry you wish to delete.
- If necessary, select another entry by keeping the "Shift" key pressed.
  All lines from the first entry selected to the last entry selected (inclusive) are selected.
- If necessary, select further entries by keeping the "Ctrl" key pressed.
  These lines are added individually to the selection.
- Click the **Delete** button.
  All selected access authorisations are immediately deleted without a confirmation prompt.

Note:
If a transponder card is held in front of the transponder reader again after the access authorisation has been deleted, a corresponding line is added at the end of the table as in the case where a new transponder card is added.

6.5.2 Filter functions

The settings in the **Filter** area allow the list of displayed access authorisations to be restricted, e.g. only for a specific user. The following settings are possible here:

Parameter	Explanation
Type	Type of access authorisation (transponder card or number code).
Code	Number of the transponder card or number code for access.
User	Selection of the user authorised for the access.

Tab. 6: Filter functions

An entry in a field indicates that a filter is active. A "Backspace" arrow is also displayed in the associated list field.

- To cancel an active filter, click the "Backspace" arrow or delete the entry in the field manually.

6.5.3 Options

In the **Options** area, two security functions can be enabled or disabled and the associated time interval specified.

Four-eyes principle

When the four-eyes principle is activated, two persons must identify themselves to open a handle or a door. To do this, two different persons must register themselves with their transponder cards or their number code within a set time interval on the same card reader.

To activate the four-eyes principle:

- Assign the "AccessAck" user to a transponder card or a number code in the "Access Configurations" dialogue.
  By default, this user is present on each Rittal embedded device and belongs to the "Access" group to which no further rights are assigned.
- If the "AccessAck" user and/or the "Access" group are not present (e.g. because prior to an update of the Rittal embedded device, all storage spaces are already occupied), you must manually create the user and the group (refer to the Rittal embedded device assembly and operating instructions).
- Set the time interval in the "Timeout" field within which the two users must register for activated four-eyes principle.

EN

After saving this assignment, the four-eyes principle governs the **complete** access control. Consequently, at least two transponder cards or two access codes are required for **each** reader unit.

To open a handle or a door:

- The first user registers himself/herself with his/her transponder code or number code on the reader unit.
- The second user registers himself/herself with his/her transponder code or number code within the set time interval on the same reader unit.

At least one of the two users must be the "AccessAck" user. The order with which the users register does not matter.

Note:
The time interval within which the two users must register can also be specified directly in the "access.cmc3" file (see section 6.7 "Manual changes to the "access.cmc3" file").

Note:
If two-factor authentication is also enabled, the four-eye mode functionality is disabled automatically. If the user "AccessAck" is (still) assigned to a handle, the associated "4 Eyes (Enabled)" checkbox is still displayed as "active".

Two-factor authentication

When two-factor authentication is enabled, two different access authorisations must be entered to open a handle or door. To do this, a transponder card must be held in front of a reader unit and a number code entered at a coded lock within a set time interval.

To enable two-factor authentication:

- Enable the "2 Factor-Authentication" entry.
- In the associated "Timeout" field, set the time interval within which the two access authorisations must be entered.

An enabled two-factor authentication applies to the entire access control. This means that a transponder card and an access code are required for each access.

To open a handle or a door:

- The user logs on to the associated reader unit with the first authentication, i.e. a transponder card or a number code.
- The user then logs on to the second assigned reader unit with their second authentication within the set time interval.

Note:
The time interval within which the user must log on with the two access authorisations can also be specified directly in the "access.cmc3" file (see section 6.7 "Manual changes to the "access.cmc3" file").

6.5.4 Assignment of reader units to access modules

By default, on input of an authorised code or holding an authorised card at a reader unit, all handles and virtual access controllers assigned to the associated access authorisation in the **Tree** group frame are opened or switched, respectively (see section 6.5.1 "Specification of the access authorisations").

Reader units and access modules can now be assigned to each other in the **Keypad Mapping** group frame. This allows you to control which handles and doors can be opened depending on the associated reader unit.

– **No assignment stored:** All access modules assigned to the associated access authorisation in the **Tree** group frame are authorised.
– **Assignment between the reader unit and the access module(s) stored:** Only those access modules assigned to the associated reader unit are authorised. These access modules must also be assigned in the **Tree** group frame as a device to the associated access authorisation.

To configure the assignment of a reader unit to specific handles and doors:

- Mark in the **Keypad Mapping** group frame the line with the access module to which the reader unit is connected, and to which you want to assign specific handles and doors.
- Click the **Edit** button.
  The "Access Configuration" dialogue opens.
- If necessary, enable a higher-level group in the tree representation (e.g. an entire "Access Control") to open all assigned handles on the reader unit.
- If necessary, disable individual handles of a group by reclicking them.

Note:
If a reader unit is not assigned to one or more handles, it is automatically assigned to **all** existing handles. In this case, all handles or doors enabled for the transponder card or the number code are opened when this reader unit is used.

6.6 Monitoring tab

All settings for the access control, such as the sensitivity of the integrated access sensor, are made on the **Monitoring** tab.

In the following sections 6.6.1 "Device" to 6.6.6 "Keypads > Keypad1 or Keypad2", only those parameters which you can modify are described. There are also display values that provide information.

6.6.1 Device

General settings for the access control are configured at the "Device" level.

Parameter	Explanation
Description	Specific description of the access control.
Location	Installation location of the access control.

Tab. 7: Settings at "Device" level

In addition, parameters that provide detailed information about the access control, such as its software and hardware versions, are also displayed. You should have such information available, in particular to enable rapid troubleshooting when requesting assistance from Rittal.

6.6.2 Access

The access sensor settings are configured on the "Access" level.

Parameter	Explanation
DescName	Specific description of the access sensor.
Command	Can be used in tasks to monitor the door status "open/closed" with an external sensor instead of the integrated infrared sensor. This requires that the value "0" must be entered for the "Sensitivity" parameter.
Sensitivity	Distance between the sensor and the door (1 = small, 3 = large) or sensor deactivated (0)
Delay	Time delay after which the status message changes.

Tab. 8: Settings at "Access" level

Note:
The "Command" parameter is set automatically to the default value "Open" when a new sensor is registered on the bus or the Rittal Embedded Device is restarted.

The following parameters are also displayed for the access sensor:

Parameter	Explanation
Value	The current value of the access sensor (0 = door closed, 1 = door open).
Status	Current status of the access sensor, taking into account the time delay.

Tab. 9: Displays at "Access" level

6.6.3 gValues

The vandalism sensor settings are configured on the "gValues" level.

Parameter	Explanation
DescName	Specific description of the vandalism sensor.
SetPtHigh-Alarm	Upper limit acceleration for which an alarm message is issued when exceeded.

Tab. 10: Settings at "gValues" level

The following parameters are also displayed for the vandalism sensor:

Parameter	Explanation
X Axis - Value	Currently measured acceleration value in X direction.
Y Axis - Value	Currently measured acceleration value in Y direction.
Z Axis - Value	Currently measured acceleration value in Z direction.
Status	Current status of the vandalism sensor, taking into account the time delay.

Tab. 11: Displays at "gValues" level

Note:
If the value "0" is entered for all limit values at the "gValues" level, the status of the vandalism sensor is always "OK".

6.6.4 Handles > Handle1 or Handle2 > Handle

Settings for the handle used are performed at the "Handle" level.

Parameter	Explanation
DescName	Specific description of the handle used.
Command	By selecting the "Unlock" entry, an electromagnetic handle can be unlocked via the Rittal embedded device website (status "Unlocked") so that it can be opened. Accordingly, a handle can be locked (status "Locked") by selecting the "Lock" entry so that it cannot be opened. By selecting the "Delay" entry, the handle is unlocked for the period of time specified in the "Delay" field and is subsequently locked again.

EN

Parameter	Explanation
Delay	Time delay after which the status message changes.

Tab. 12: Settings at "Handle" level

The following parameters are also displayed for the handle used:

Parameter	Explanation
Value	Current status of the handle used (0 = handle closed, 1 = handle open).
Status	Current locking status.

Tab. 13: Displays at "Handle" level

Note:
The logic above for the "Value" parameter applies to handles DK 7030.610 and DK 7030.611. The logic may be inverted for other handle systems (0 = handle open, 1 = handle closed).

Note:
There is no error message if the handle is disconnected from the access control. The handle status changes to "Inactive" and a corresponding message is generated in the log information. The status change can be queried in a task and linked with an action.

Note:
If the handle is opened with a master key, the Rittal embedded device displays an alarm message. This can be eliminated again by closing the handle.

6.6.5 Handles > Handle1 or Handle2 > LED

The settings for the LED display in the handle are configured at the "LED" level.

Parameter	Explanation
Mode	Control of the LED display in the handle. "Off": LED display switched off permanently. "Access": Display in accordance with the switching status of the handle or the status of the access control. "Access & beeper": Similar to "Access", an acoustic signal also sounds in the event of a fault. "CMC": Display in accordance with the status of the Rittal embedded device. "CMC & beeper": Similar to "CMC", an acoustic signal also sounds in the event of a fault. "Task": Display in accordance with the evaluation of a task ("LED.Command" variable). "Task & beeper": Similar to "Task", an acoustic signal also sounds in the event of a fault.
Command	The colour of the LED can be set when the "Task" mode is selected. The colour is retained until the task is next initiated. If "Custom" is selected, the colour can be defined using the three components: red, green and blue.
Red	Red component of the colour.
Green	Green component of the colour.
Blue	Blue component of the colour.

Tab. 14: Settings at the "LED" level

6.6.6 Keypads > Keypad1 or Keypad2

The settings for the coded lock and transponder reader are configured at the "KeyPad" level.

Parameter	Explanation
DescName	Specific description of the coded lock or transponder reader used.
Command	Selecting the "On" entry activates the connected coded lock or the transponder reader. Accordingly, a connected reader unit can be deactivated by selecting the "Off" entry so that it **cannot** be used to open the door.

Tab. 15: Settings at "KeyPad" level

The following parameters are also displayed for the coded lock/transponder reader:

Parameter	Explanation
Status	Indicates whether a coded lock or transponder reader has been connected (active) or not (inactive), or the reader unit has been deactivated (off).

Tab. 16: Displays at "KeyPad" level

6.7 Manual changes to the "access.cmc3" file

Alternatively, the access authorisation settings can also be made directly in the "access.cmc3" file. This file is created automatically in the "upload" directory of the Rittal embedded device when it is started for the first time.

Note:
If the "access.cmc3" file is removed from the folder, access is only then possible using the three predefined access codes "1001", "1002" and "1003". All other access authorisations have to initially be added again to a newly created file.

6.7.1 Downloading the file

Note:
The following descriptions assume that you establish an (S)FTP connection using the "FileZilla" program. If another program is used, the file may have to be downloaded and uploaded in a different way.

- First establish an FTP or SFTP connection to the Rittal embedded device from a PC (see the assembly and operating instructions for the Rittal embedded device).
- In the left-hand subwindow (PC), switch to the folder where you wish to locally save the "access.cmc3" file.
- Switch to the "upload" folder in the right-hand subwindow (Rittal Embedded Device).
- Right-click the "access.cmc3" file and select the "Download" action.
- Disconnect the (S)FTP connection between the PC and Rittal embedded device.

If there is no "access.cmc3" file in the "upload" directory, this has to be created first.

- When using a coded lock: Input any sequence of numbers on the coded lock and confirm using the "Enter" key.
  The file is now generated in the "upload" folder.
- When using a transponder reader: Hold any transponder card in front of the reader unit.
  The file is now generated in the "upload" folder.
- Establish an (S)FTP connection between the PC and Rittal embedded device again and download the file.
- Disconnect the (S)FTP connection between the PC and Rittal embedded device again.

6.7.2 Editing the file

The file can now be edited using a text editor. Rittal recommends using "Notepad++" for this instead of the standard "Notepad" editor installed under Windows. This is available online as freeware.

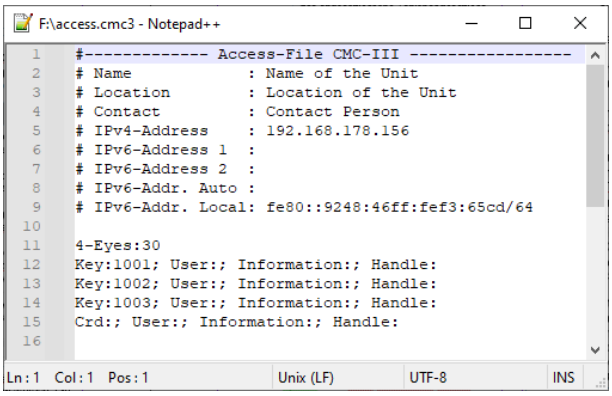

Fig. 15: "access.cmc3" file in Notepad++

The file is structured as follows:

- Lines starting with a "#" are comment lines. These contain basic information on the Rittal Embedded Device.
- Lines with "Key" or "Crd" as first entry contain the authorised access codes if a numeric coded lock is used, or the authorised card numbers of the transponder cards if a transponder reader is used (see section 6.5.1 "Specification of the access authorisations").
- The line with "4-Eyes" as first entry contains the time interval for the registration in the four-eyes principle (see section 6.5.3 "Options").
- Lines with "Keypad" as first entry contain the assignment of reader units to individual access modules (see section 6.5.4 "Assignment of reader units to access modules").

Access codes and transponder cards

The lines for the access codes and the transponder cards contain the following entries:

Parameter	Explanation
Key	Access code containing up to eight digits for a coded lock for authorised access.
Crd	Card number of a transponder card for authorised access.
User	User to be entered in the Rittal embedded device logfile when the coded lock is opened with the associated access code or on opening with the associated transponder card. This user has to exist in the Rittal embedded device.
Information	Specific additional information for the access. This text is also added for the user in the Rittal embedded device logfile.

EN

Parameter	Explanation
Handle	Serial number of the access control or (virtual) access controller to which the access module to be switched is connected. Several comma-separated entries for different access control units can also be added here.

Tab. 17: Entries for access codes and transponder cards

Note:
Each line contains the parameter "Key" or "Crd" depending on whether the line applies to a coded lock or transponder reader.

The entries are explained in detail using the following example configuration.

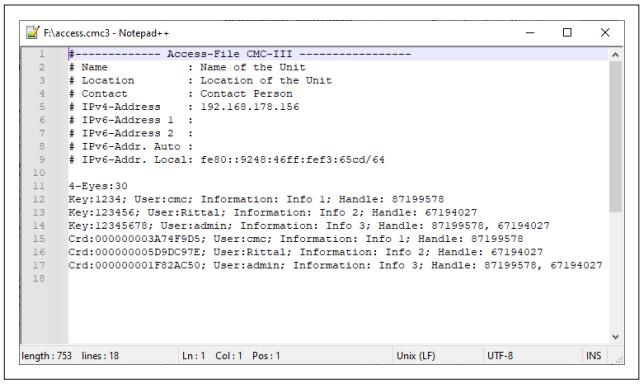

Fig. 16: Example configuration

The file is structured as follows:

– Handle 1 is opened using access code "1234" (line 11 in the editor window). User "cmc" and the information "Info 1" are entered in the Rittal embedded device logfile.
– Handle 2 is opened using access code "123456" (line 12). User "Rittal" and the information "Info 2" are entered in the Rittal embedded device logfile.
– Both handles are opened using access code "12345678" (line 13). User "admin" and the information "Info 3" are entered in the Rittal embedded device logfile.

In lines 15 to 17, a transponder card has also been assigned to each of the users. These transponder cards open the same handles as the access codes above. The respective users and associated information are entered in the Rittal embedded device logfile logfile.

Time interval for the four-eyes principle

The time interval for registration in the four-eyes principle is specified in the line with the "4-Eyes" entry.

Parameter	Explanation
4-Eyes	Time interval in seconds within which the two persons must register with their transponder cards or their number code.

Tab. 18: Time interval for the four-eyes principle

Assignment of reader units to access modules

The lines for the assignment of reader units to access codes contain the following entries:

Parameter	Explanation
Keypad	Serial number of the access control or the (virtual) access controller to which the reader unit is connected with the following assigned handles or doors.
Handle	Serial number of the access control or (virtual) access controller to which the access module to be switched is connected. Several comma-separated entries for different access control units can also be added here.

Tab. 19: Assignment of reader units to access modules

Note:
If **no** access module is assigned to the "Handle" entry, the reader unit will be assigned to **all** access modules. In this case, all doors activated for the transponder card or the number code will be opened, irrespective of which reader unit is used.

6.7.3 Uploading the file

Once all entries have been made in the "access.cmc3" file, this file has to be stored in the "upload" directory on the Rittal embedded device again.

- Establish an FTP or SFTP connection to the Rittal embedded device from a PC again.
- Switch to the "upload" folder in the right-hand subwindow (Rittal embedded device).
- In the left-hand subwindow (PC), switch to the folder where you have stored the revised version of the "access.cmc3" file.
- Right-click the "access.cmc3" file and select the "Upload" action.
- If the file cannot be uploaded this way, first delete the existing "access.cmc3" file from the "upload" directory and then upload the file from the PC again.
- Finally, disconnect the (S)FTP connection between the PC and Rittal embedded device.

The access authorisations have now been updated.

7 Storage and disposal

7.1 Storage

If the device is not used for a long period, Rittal recommends that it be disconnected from the mains power supply and protected from damp and dust.

7.2 Disposal

Since the access control consists mainly of the "housing" and "circuit board" parts, the device must be passed on to the electronic waste recycling system for disposal.

EN

8 Technical specifications

Technical specifications		DK access control
Model no.		7010.180
W x H x D (mm)		110 x 30 x 40
Operating temperature range		0 °C…+55 °C
Storage temperature		-20 °C…+70 °C
Operating humidity range		5%…95% relative humidity, non-condensing
Mode of operation		optical
Transmitter		Infrared diode
Receiver		Infrared receiver
Protection category		IP 30 to IEC 60 529
Inputs and outputs	CAN bus (RJ 45)	2 x
	Handle (RJ 12)	2 x
	Connection for CMC III reader unit	2 x
Operation/signals	LED display	OK/warning/alarm/CAN bus status

Tab. 20: Technical specifications

EN

9 Customer service addresses

For technical queries, please contact:
Tel.: +49(0)2772 505-9052
E-mail: info@rittal.de
Homepage: www.rittal.de

For complaints or service requests, please contact:
Tel.: +49(0)2772 505-1855
E-mail: service@rittal.de

Contact details can be found on the Rittal website at:
– https://www.rittal.com/rittal-locations

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-EN

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