

product description

desktop and wall box made from plastic for an RF1000 reader

SIMATIC RF1000 desktop and wall box for all access control readers of the RF10x0R family



Technical Product Detail Page

<https://i.siemens.com/1P6GT2890-0CB00>

suitability for use

enclosure for placing on a table with rubber feet or mounting on the wall with screws

suitability for operation

for RF1040R, RF1060R, RF1070R

mechanical data

material

Polycarbonate

color

Ti gray

ambient conditions

ambient temperature

- during operation -25 ... +55 °C
- during storage -40 ... +85 °C
- during transport -40 ... +85 °C

design, dimensions and weights

width

121 mm

height

24.5 mm

depth

75.7 mm

net weight

58 g

standards, specifications, approvals

reference code

- according to IEC 81346-2:2019 UCA

further information / internet links

internet link

- to website: Selection guide for cables and connectors <https://support.industry.siemens.com/cs/ww/en/view/109766358>
- to web page: selection aid TIA Selection Tool <https://www.siemens.com/tstcloud>
- to website: Industrial communication <https://www.siemens.com/simatic-net>
- to web page: SiePortal <https://sieportal.siemens.com/>
- to website: Image database <https://www.automation.siemens.com/bilddb>
- to website: CAx-Download-Manager <https://www.siemens.com/cax>
- to website: Industry Online Support <https://support.industry.siemens.com>

Security information

security information

Siemens provides products and solutions with industrial cybersecurity functions that support the secure operation of plants, systems, machines and networks. In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial cybersecurity concept. Siemens' products and solutions constitute one element of such a concept. Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial

cybersecurity measures that may be implemented, please visit www.siemens.com/cybersecurity-industry. Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats. To stay informed about product updates, subscribe to the Siemens Industrial Cybersecurity RSS Feed under <https://www.siemens.com/cert>. (V4.7)

last modified:

10/30/2025 