

descrizione del prodotto

cassetta da tavolo/cassetta da parete in plastica per un Reader RF1000

SIMATIC RF1000 cassetta da tavolo e da parete per tutti gli Access Control Reader della famiglia RF10x0R



pagina di informazioni tecniche sul prodotto

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

idoneità all'impiego

custodia da appoggio su tavolo con piedini in gomma o per montaggio a parete con viti

idoneità all'impiego

per RF1040R, RF1060R, RF1070R

dati meccanici

materiale

polycarbonato

colore

grigio titanio

condizioni ambientali

temperatura ambiente

- durante l'esercizio -25 ... +55 °C
- durante l'immagazzinaggio -40 ... +85 °C
- durante il trasporto -40 ... +85 °C

forma costruttiva, dimensioni e pesi

larghezza

121 mm

altezza

24,5 mm

profondità

75,7 mm

peso netto

58 g

norme, specifiche, omologazioni

codice di riferimento

- secondo IEC 81346-2:2019

UCA

ulteriori informazioni / links Internet

link Internet

- alla pagina web: Guida alla scelta di cavi e connettori
- alla pagina web: supporto per la scelta TIA Selection Tool
- alla pagina web: Comunicazione industriale
- alla pagina web: SiePortal
- alla pagina web: Banca dati di immagini
- alla pagina web: Download Manager CAX
- alla pagina web: Industry Online Support

<https://support.industry.siemens.com/cs/ww/de/view/109766358>
<https://www.siemens.com/tstcloud>
<https://www.siemens.com/simatic-net>
<https://sieportal.siemens.com/>
<https://www.automation.siemens.com/bilddb>
<https://www.siemens.com/cax>
<https://support.industry.siemens.com>

Indicazioni di sicurezza

avvertenze di security

Siemens commercializza prodotti e soluzioni dotati di funzioni di cybersecurity industriale che contribuiscono al funzionamento sicuro di impianti, soluzioni, macchine e reti. Al fine di proteggere impianti, sistemi, macchine e reti da minacce cibernetiche, è necessario implementare - e mantenere continuamente - un concetto di cybersecurity industriale globale ed all'avanguardia. I prodotti e le soluzioni Siemens costituiscono soltanto una componente di questo concetto. È responsabilità dei clienti prevenire accessi non autorizzati ai propri impianti, sistemi, macchine e reti. Tali sistemi, macchine e componenti dovrebbero essere connessi unicamente a una rete aziendale o a Internet se e nella misura in cui detta connessione sia necessaria e solo quando siano attive appropriate misure di sicurezza (ad es. impiego di

firewall e segmentazione della rete). Per ulteriori informazioni inerenti alle misure di cybersecurity industriale che possono essere implementabili potete visitare il sito www.siemens.com/cybersecurity-industry. I prodotti e le soluzioni Siemens vengono costantemente perfezionati per incrementarne la sicurezza. Siemens raccomanda espressamente che gli aggiornamenti dei prodotti siano effettuati non appena disponibili e che siano utilizzate le versioni più aggiornate. L'utilizzo di versioni di prodotti non più supportate ed il mancato aggiornamento degli stessi incrementa il rischio di attacchi cibernetici. Per essere informati riguardo agli aggiornamenti dei prodotti, potete iscrivervi a Siemens Industrial Cybersecurity RSS Feed al sito <https://www.siemens.com/cert>. (V4.7)

Ultima modifica:

30/10/2025 