SIEMENS

Data sheet 6GT2891-7UH18

product type designation	**Plug-in cable RS232, D-sub-D /USB-A / PicoBlade**
product description	flexible communication line
	SIMATIC RF1000 RS232 plug-in cable for RF1000 reader to PC with D-sub 9-pin plug, 5 V via USB A plug, length 1.8 m consisting of 6GT2891-7UA18, 6GT2091-7UH10.
product brand name	SIMATIC RF
Technical Product Detail Page	https://i.siemens.com/1P6GT2891-7UH18
suitability for use	Plug-in cable for connecting an RF1000 reader to a PC or other serial modules with submin D connection
wire length	1.8 m
electrical data	
number of electrical connections	3
type of electrical connection	submin-D (female, 9-pole, straight) / USB-A / PicoBlade 51021 5-pole
mechanical data	
number of electrical cores	5
outer diameter	
● of cable sheath	5 mm
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 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)
Approvals / Certificates	
General Product Approval	

EAC

last modified: 6/28/2026

Subject to change without notice
© Copyright Siemens