SIEMENS

Data sheet 6GK5798-8MS00-0AA0

product type designation	**Mounting kit for SCALANCE W1780, rail mounting**
	Mounting kit for SCALANCE W1780 mounting bar installation can only be used in connection with SCALANCE W1788/W1788EEC/ W1748; for S7-300 / S7-1500 mounting rail scope of delivery: 1 mounting adapter fixing screws.


Technical Product Detail Page	https://i.siemens.com/1P6GK5798-8MS00-0AA0
mechanical data	
material	Stainless steel
color	metallic
design, dimensions and weights	
design	2 mounting plates plus mounting material
width	26 mm
height	67 mm
depth	5.25 mm
net weight	22 g
design of the screw head / slot	Yes; 2 units of 2.9x 16 (profile screw)
design of the screw head / torx	Yes; 2 units: M4x8 (mounting screws)
standards, specifications, approvals	
certificate of suitability	
● RoHS conformity	Yes
reference code	
● according to IEC 81346-2:2019	UQB
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 the website: IWLAN	https://www.siemens.com/iwlan
● 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
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