

SCALANCE CLP 32 GB removable data storage medium for simple device replacement in case of failure, for recording configuration data or as memory expansion, can be used in the following products with CLP slot



product type designation	
product type designation	SCALANCE CLP 32GB
Technical Product Detail Page	https://i.siemens.com/1P6GK1900-0UB40-0AA0
suitability for operation	SCALANCE devices with CLP slot
ambient conditions	
ambient temperature	
<ul style="list-style-type: none"> during operation during storage during transport 	-40 ... +85 °C
relative humidity	
<ul style="list-style-type: none"> at 25 °C / without condensation / during operation / maximum 	95 %
protection class IP	IP20
design, dimensions and weights	
width	17.5 mm
height	7 mm
depth	32 mm
net weight	3.1 g
product feature / conformal coating	No
product features, product functions, product components / general	
storage capacity	32768 Mibyte
standards, specifications, approvals	
MTBF	343 a
range of validity / for MTBF determination	at 25 °C
further information / internet links	
internet link	
<ul style="list-style-type: none"> to web page: selection aid TIA Selection Tool to website: Industrial communication to web page: SiePortal to website: Image database to website: CAx-Download-Manager to website: Industry Online Support 	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
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



[Manufacturer Declaration](#)

[China RoHS](#)



last modified:

1/12/2026 