








SCALANCE XB108-2 unmanaged IE switch, 8x 10/100 Mbit/s Ports, 2x 100 Mbit/s multimode BFOC, for setting up small star and line topologies, LED diagnostics, IP20, redundant power supply 24 V AC/DC Manual available as a download .

product type designation	
product brand name	SCALANCE
product type designation	XB108-2
transfer rate	
transfer rate	10 Mbit/s, 100 Mbit/s
interfaces / for communication / integrated	
number of electrical connections • for network components or terminal equipment	8; RJ45
number of 100 Mbit/s ST(BFOC) ports • for multimode	2
transmission method / of the optical interface	100BaseFX
interfaces / other	
number of electrical connections • for power supply	1
supply voltage, current consumption, power loss	
product component / connection for redundant voltage supply	Yes
type of voltage / 1 / of the supply voltage	DC
• supply voltage / 1 / rated value	24 V
• power loss [W] / 1 / rated value	7.2 W
• supply voltage / 1 / rated value	19.2 ... 28.8 V
• consumed current / 1 / maximum	0.3 A
• product component / 1 / fusing at power supply input	Yes
• fuse protection type / 1 / at input for supply voltage	0.6 A / 60 V
type of voltage / 2 / of the supply voltage	AC
• supply voltage / 2 / rated value	19.2 ... 28.8 V
ambient conditions	
ambient temperature	
• during operation	0 ... 60 °C
• during storage	-40 ... +80 °C
• during transport	-40 ... +80 °C
relative humidity	
• at 25 °C / without condensation / during operation / maximum	95 %
protection class IP	IP20
design, dimensions and weights	
design	compact
width	80 mm
height	117 mm
depth	109 mm
net weight	0.34 kg

fastening method	
<ul style="list-style-type: none"> • 35 mm top hat DIN rail mounting • wall mounting • S7-300 rail mounting • S7-1500 rail mounting 	<p>Yes</p> <p>No</p> <p>No</p> <p>No</p>
product functions / management, configuration, engineering	
product function	
<ul style="list-style-type: none"> • multiport mirroring • CoS • switch-managed 	<p>No</p> <p>Yes</p> <p>No</p>
PROFINET conformity class	A
product functions / redundancy	
product function	
<ul style="list-style-type: none"> • Parallel Redundancy Protocol (PRP)/operation in the PRP-network • Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA) 	<p>Yes</p> <p>No</p>
standards, specifications, approvals	
certificate of suitability	
<ul style="list-style-type: none"> • CE marking • cULus approval • KC approval • Regulatory Compliance Mark (RCM) 	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>
standard	
<ul style="list-style-type: none"> • for safety / from CSA and UL 	UL 60950-1, CSA C22.2 No. 60950-1
standards, specifications, approvals / hazardous environments	
certificate of suitability	
<ul style="list-style-type: none"> • ATEX • UKEX • IECEx • ULhazloc approval • CCC / for hazardous zone according to GB standard • FM registration 	<p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p> <p>Yes</p>
standards, specifications, approvals / other	
certificate of suitability	
<ul style="list-style-type: none"> • RoHS conformity 	Yes
product functions / general	
MTBF	71 a
reference code	
<ul style="list-style-type: none"> • according to IEC 81346-2 • according to IEC 81346-2:2019 	<p>KF</p> <p>KFE</p>
Warranty period	5 a
further information / internet links	
internet link	
<ul style="list-style-type: none"> • to website: Image database • to website: Industry Online Support 	<p>https://www.automation.siemens.com/bilddb</p> <p>https://support.industry.siemens.com</p>
security information	
security information	<p>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)</p>

Approvals / Certificates

General Product Approval	EMV	For use in hazardous locations
 EG-Konf.	Declaration of Conformity	 UL
 RCM	KC	 IECEX
For use in hazardous locations	Environment	Industrial Communication
 ATEX	FM	CCC-Ex
	Confirmation	PROFINET

last modified:

4/24/2024 