



SCALANCE XF204 managed two BusAdapters BA 2xRJ45 HA IEC 62443-4-2 certified; IE switch, 4 x 10/100 Mbps, 2 x BusAdapter interface, error signaling contact, set pushbutton, redundant 24 V DC power supply, PROFINET device, extended temperature range -40 °C...+70 °C, conformal coating, with electronic manual on DVD, C-PLUG optional, delivery with BusAdapter. 6DL1193-6AR00-0AA0

product type designation	
product brand name	SCALANCE
product type designation	XF204
Technical Product Detail Page	https://i.siemens.com/1P6GK5204-0BA00-2GF2
transfer rate	
transfer rate	10, 100 Mbit/s
interfaces / for communication / integrated	
number of electrical connections	
• for network components or terminal equipment	4
interfaces / other	
number of electrical connections	
• for signaling contact	1
• for power supply	1
type of electrical connection	
• for signaling contact	2-pole terminal block
• for power supply	2-pole terminal block
design of the removable storage	
• C-PLUG	Yes
operating voltage / of the signaling contacts	
• at DC / rated value	24 V
operational current / of the signaling contacts	
• at DC / maximum	0.1 A
supply voltage, current consumption, power loss	
product component / connection for redundant voltage supply	Yes
type of voltage / 1 / of the supply voltage	
• supply voltage / 1 / rated value	24 V
• power loss [W] / 1 / rated value	8.6 W
• supply voltage / 1 / voltage range	19.2 ... 28.8
• consumed current / 1 / maximum	0.36 A
• type of electrical connection / 1 / for power supply	2-pole terminal block
• product component / 1 / fusing at power supply input	Yes
• fuse protection type / 1 / at input for supply voltage	2.5 A (cannot be replaced by user)
ambient conditions	
ambient temperature	
• during operation	-40 ... +70 °C
• during storage	-40 ... +85 °C
• during transport	-40 ... +85 °C
relative humidity	
• at 25 °C / without condensation / during operation /	95 %

maximum	
protection class IP	IP20
design, dimensions and weights	
design	compact
width	100 mm
height	117 mm
depth	74 mm
net weight	0.25 kg
fastening method	
• 35 mm DIN-rail mounting	Yes
• wall mounting	No
• S7-300 rail mounting	No
• S7-1500 rail mounting	No
product features, product functions, product components / general	
cascading in the case of a redundant ring / at reconfiguration time of <1~0.31~s	50
cascading in cases of star topology	any (depending only on signal propagation time)
product functions / management, configuration, engineering	
product function	
• CLI	Yes
• web-based management	Yes
• MIB support	Yes
• TRAPs via email	Yes
• configuration with STEP 7	Yes
• port mirroring	Yes
• multiport mirroring	Yes
• PROFINET IO diagnosis	Yes
• switch-managed	Yes
PROFINET conformity class	B
protocol / is supported	
• Telnet	Yes
• HTTP	Yes
• HTTPS	Yes
• TFTP	Yes
• FTP	No
• BOOTP	No
• DCP	Yes
• LLDP	Yes
• SNMP v1	Yes
• SNMP v2	Yes
• SNMP v3	Yes
identification & maintenance function	
• I&M0 - device-specific information	Yes
• I&M1 - higher level designation/location designation	Yes
product functions / diagnostics	
product function	
• port diagnostics	Yes
• statistics Packet Size	Yes
• statistics packet type	Yes
• error statistics	Yes
product functions / DHCP	
product function	
• DHCP client	Yes
product functions / redundancy	
protocol / is supported / Media Redundancy Protocol (MRP)	Yes
product function	
• media redundancy protocol (MRP) with redundancy manager	Yes
• Media Redundancy Protocol Interconnection (MRP-I)	Yes

<ul style="list-style-type: none"> Media Redundancy Protocol for Planned Duplication (MRPD) of the PROFINET IO device / is supported / H-Sync forwarding of the PROFINET IO device / is supported / PROFINET system redundancy ring redundancy high speed redundancy protocol (HRP) with redundancy manager high speed redundancy protocol (HRP) with standby redundancy redundancy procedure RSTP+ Parallel Redundancy Protocol (PRP)/operation in the PRP-network Parallel Redundancy Protocol (PRP)/Redundant Network Access (RNA) passive listening 	No Yes Yes Yes Yes Yes No No Yes
product functions / security	
protocol / is supported	
<ul style="list-style-type: none"> SSH 	Yes
product functions / time	
product function	
<ul style="list-style-type: none"> SICLOCK support 	No
protocol / is supported	
<ul style="list-style-type: none"> NTP SNTP 	No Yes
standards, specifications, approvals	
certificate of suitability	
<ul style="list-style-type: none"> CE marking KC approval 	Yes Yes
standard	
<ul style="list-style-type: none"> for EMC interference emission for immunity to EMC for safety / from CSA and UL 	EN 61000-6-4:2001 (Class A) EN 61000-6-2, EN 61000-6-4 UL 61010-2-201
standards, specifications, approvals / other	
certificate of suitability	
<ul style="list-style-type: none"> railway application in accordance with EN 50124-1 	No
IT security for industrial automation systems / according to IEC 62443-4-2:2019	Yes
product functions / general	
warranty period	5 a
further information / internet links	
internet link	
<ul style="list-style-type: none"> to website: Selection guide for cables and connectors 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://support.industry.siemens.com/cs/ww/en/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
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</p>

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



[Miscellaneous](#)

[Declaration of Con-
formity](#)

last modified:

12/15/2025