

product type designation

product description



IWLAN Access Point

IWLAN Access Point, SCALANCE WAB762-1 1 radio, 1 R-SMA antenna port, IEEE 802.11ax, 2.4/5 GHz, gross data rate 601 Mbps, 1x RJ45 max. 1000 Mbps, 24 V DC, joint block, IP20, 0... +55 °C, . observe national approvals! CERT ID: ELAX-W1-RJ-E1, scope of delivery: safety instructions German/English, 1x joint block; for operation outside of USA/Israel

suitability for use

www.siemens.com/iwlan

transfer rate

transfer rate

- with WLAN / maximum
- for Industrial Ethernet

601 Mbit/s
10, 100, 1000 Mbit/s

interfaces

number of electrical/optical connections / for network components or terminal equipment / maximum / note

1

number of electrical/optical connections / for gigabit Ethernet / maximum

1

number of electrical connections

- for network components or terminal equipment
- for power supply
- for redundant voltage supply

1
1
0

type of electrical connection

- for network components or terminal equipment
- for power supply

RJ45 socket
3-pin terminal block

memory

design of the removable storage

- CLP
- CLP iFeatures

No
No

interfaces / wireless

number of radio cards / permanently installed

1

transmission mode / for multiple input multiple output (MIMO)

1x1

number of spatial streams

1

number of electrical connections / for external antenna(s)

1

type of electrical connection / for external antenna(s)

R-SMA (socket)

product feature / external antenna can be mounted directly on device

Yes

signal inputs/outputs

number of digital inputs

0

number of digital outputs

0

product functions / management, configuration, engineering

product function / is supported / identification link

Yes; acc. to IEC 61406-1:2022

standards, specifications, approvals

reference code

- according to IEC 81346-2:2019

KFE

standards, specifications, approvals / Environmental Product Declaration

Environmental Product Declaration

Yes

global warming potential [CO2 eq]	
<ul style="list-style-type: none"> • total • during manufacturing • during operation • after end of life 	<p>200.91 kg</p> <p>12.97 kg</p> <p>187.77 kg</p> <p>0.17 kg</p>





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 web page: WLAN country approval • to the website: IWLAN • to website: Industrial communication • to web page: SiePortal • to website: Image database • to website: CAx-Download-Manager • to website: Industry Online Support 	<p>https://support.industry.siemens.com/cs/ww/en/view/109766358</p> <p>https://www.siemens.com/tstcloud</p> <p>https://www.siemens.com/wireless-approvals</p> <p>https://www.siemens.com/iwlan</p> <p>https://www.siemens.com/simatic-net</p> <p>https://sieportal.siemens.com/</p> <p>https://www.automation.siemens.com/bilddb</p> <p>https://www.siemens.com/cax</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	Radio Equipment Type Approval Certificate
   	<p>Type Examination Certificate</p> <p>Miscellaneous</p>

Environment



last modified:

8/7/2025 