LCOS 10.94

R&S®LANCOM IAP-5G

Secure SD-WAN over 5G for harsh environments

This Secure SD-WAN gateway is the ideal solution for reliable and high-performance 5G Internet in tough environments such as in warehousing and logistics, or for covered outdoor areas without a wired Internet connection. The extremely robust housing is highly dustproof and is suitable for temperatures from -20 to +50°C. With integrated VPN functionality via IPSec and WireGuard and an integrated 5G modem, this device provides professional site connectivity via cellular networking and fast data transfer—ideal for connecting automated systems, machines, and surveillance equipment.

- Integrated 5G modem for low latency and high bandwidth for real-time applications
- Robust IP50 all-metal housing for maximum reliability in harsh environments
- Reliable even at demanding temperatures (-20°C to +50°C)
- Flexible power supply via Power over Ethernet (PoE) according to IEEE 802.3at
- Secure site connectivity with 5 simultaneous VPN connections (25 channels optional)
- Integrated stateful-inspection firewall with intrusion detection and Denial-of-Service protection
- Network virtualization with up to 16 networks on one device (ARF)
- Extended protection with the content filter of the R&S®LANCOM Security Essentials Option

R&S®LANCOM IAP-5G

Fully future-proof with 5G

With the R&S®LANCOM IAP-5G, you benefit from all the advantages of the high-performance 5G mobile communications standard. With low latency and high bandwidth for the use of real-time applications even with a high user density, it offers a professional and secure high-speed Internet connection for locations without wired Internet line availability.

Robust all-metal housing

The durable metal housing allows this cellular router to guarantee excellent Internet connections even in tough and dusty environments. It protects the R&S®LANCOM IAP-5G from external influences and is ideal for use in warehouses or indoor event venues. Thanks to an extended temperature range from -20°C to +50°C, the device provides reliable wireless connections under the most demanding conditions.

R&S®LANCOM SD-WAN – Next-level networking

With R&S®LANCOM SD-WAN you can manage and monitor your entire corporate network centrally, cost-effectively, quickly, and stress-free! In combination with the R&S®LANCOM Management Cloud, the SD-WAN gateway gives you all the options for an automated setup of secure VPN connections (Auto-VPN) between sites, including network virtualization. Highlight features such as High Scalability VPN (HSVPN) and Advanced Mesh VPN offer you a significant plus in scalability and efficiency for a large number of branches and applications. Furthermore, if multiple WAN connections are defined, they are automatically operated in active/active mode (load balancing), thereby increasing the available total bandwidth. With Dynamic Path Selection and Dynamic Traffic Steering, applications are also dynamically routed via the best connection at any given time.

Secure site connectivity via VPN

With virtual private networks (VPN), you use the public medium of the Internet as a communication path and secure the connection in such a way that the communication still remains completely inaccessible to external parties. This SD-WAN gateway offers you five integrated IPSec VPN channels for secure encryption, so that the protection of internal company data is always guaranteed when connecting mobile employees, home offices, or branch offices. With the R&S®LANCOM VPN Option, you can also upgrade the device to up to 25 VPN channels, so that the infrastructure can easily grow with your needs without additional hardware.

Maximum data security from its integrated firewall

Equipped with a stateful inspection firewall, the R&S®LANCOM IAP-5G protects the entire network. With features such as intrusion prevention and Denial-of-Service protection, this device provides optimal protection and secures all of the data on the network.Maximum data security from the integrated firewall.

R&S®LANCOM IAP-5G

Layer 2 features	
VLAN	4.096 IDs based on IEEE 802.1q, dynamic assignment
Multicast	IGMP-Snooping, MLD-Snooping
Protocols	ARP-Lookup, LLDP, ARP, Proxy ARP, BOOTP, DHCP
Layer 3 features	
Firewall	Stateful inspection firewall including paket filtering, extended port forwarding, N:N IP address mapping, paket tagging, support for DNS targets, user-defined rules and notifications
Quality of Service	Traffic shaping, bandwidth reservation, DiffServ/TOS, packetsize control, layer-2-in-layer-3 tagging, support for 8 QoS queues (6 free configurable)
Security	Intrusion Prevention, IP spoofing, access control lists, Denial of Service protection, detailed settings for handling reassembly, session-recovery, PING, stealth mode and AUTH port, URL blocker, password protection, programmable reset button
PPP authentication mechanisms	PAP, CHAP, MS-CHAP, and MS-CHAPv2
High availability / redundancy	VRRP (Virtual Router Redundancy Protocol)
Router	IPv4-, IPv6-, IPv4/IPv6 dual stack
SD-WAN Application Routing	SD-WAN Application Routing in connection with the R&S®LANCOM Management Cloud
SD-WAN dynamic path selection	SD-WAN dynamic path selection in connection with the R&S®LANCOM Management Cloud
SD-WAN Zero Touch Deployment	Zero touch commissioning of the device in conjunction with the R&S®LANCOM Management Cloud
Router virtualization	ARF (Advanced Routing and Forwarding) up to separate processing of 16 contexts
IPv4 services	HTTP and HTTPS server for configuration by web interface, DNS client, DNS server, DNS relay, DNS proxy, dynamic DNS client, DHCP client, DHCP relay and DHCP server including autodetection, NTP client, SNTP server, policy-based routing, Bonjour-Proxy, RADIUS
IPv6 services	HTTP and HTTPS server for configuration by web interface, DHCPv6 client, DHCPv6 server, DHCPv6 relay, DNS client, DNS server, dynamic DNS client, NTP client, SNTP server, Bonjour-Proxy, RADIUS
Dynamic routing protocols	RIPv2, BGPv4, OSPFv2, LISP (Locator/ID Separation Protocol)
IPv4 protocols	DNS, HTTP, HTTPS, ICMP, NTP/SNTP, PPPoE (server), RADIUS, RADSEC (secure RADIUS), RTP, SNMPv1,v2c,v3, TFTP, TACACS+, IGMPv3
IPv6 protocols	NDP, stateless address autoconfiguration (SLAAC), stateful address autoconfiguration (DHCPv6), router advertisements, ICMPv6, DHCPv6, DNS, HTTP, HTTPS, PPPoE, RADIUS, SMTP, NTP, Syslog, SNMPv1,v2c,v3, MLDv2, NPTv6 (NAT66), VRRPv3
WAN operating mode	VDSL, ADSL1, ADSL2 or ADSL2+ additional with external DSL modem at an ETH port
WAN protocols	PPPoE, Multi-PPPoE, GRE, EoGRE, PPTP (PAC or PNS), L2TPv2 (LAC or LNS), L2TPv3 with Ethernet-Pseudowire and IPoE (using DHCP or no DHCP), RIP-1, RIP-2, VLAN, IPv6 over PPP (IPv6 and IPv4/IPv6 dual stack session), IP(v6)oE (autokonfiguration, DHCPv6 or static)
Tunneling protocols (IPv4/IPv6)	6to4, 6in4, 6rd, Dual Stack Lite, 464XLAT
Security	
Intrusion Prevention	Monitoring and blocking of login attempts and port scans
IP spoofing	Source IP address check on all interfaces: only IP addresses belonging to the defined IP networks are allowed
Access control lists	Filtering of IP or MAC addresses and preset protocols for configuration access
Denial of Service protection	Protection from fragmentation errors and SYN flooding
General	Detailed settings for handling reassembly, PING, stealth mode and AUTH port
Password protection	Password-protected configuration access can be set for each interface
Two-factor authentication	Two-factor authentication (2FA) for local device management via WEBconfig, SSH or Telnet with external Authenticator application

R&S®LANCOM IAP-5G

Security	
Alerts	Alerts via e-mail, SNMP traps and SYSLOG
Authentication mechanisms	EAP-TLS, EAP-TTLS, PEAP, MS-CHAP, MS-CHAPv2 as EAP authentication mechanisms, PAP, CHAP, MS-CHAP and MS-CHAPv2 as PPP authentication mechanisms
Adjustable reset button	Adjustable reset button for 'ignore', 'boot-only' and 'reset-or-boot'
High availability / redundancy	
VRRP	VRRP (Virtual Router Redundancy Protocol VRRPv2 and VRRPv3) for backup in case of failure of a device or remote station.
FirmSafe	For completely safe software upgrades thanks to two stored firmware versions, incl. test mode for firmware updates
5G backup	In case of failure of the main connection, a backup connection is established over the internal 5G modem; automatic return to the main connection
Load balancing	Static and dynamic load balancing over up to 2 WAN connections. Channel bundling with Multilink PPP (if supported by network operator)
VPN redundancy	Backup of VPN connections across different hierarchy levels, e.g. in case of failure of a central VPN concentrator and re-routing to multiple distributed remote sites. Any number of VPN remote sites can be defined (the tunnel limit applies only to active connections). Up to 32 alternative remote stations, each with its own routing tag, can be defined per VPN connection. Automatic selection may be sequential, or dependant on the last connection, or random (VPN load balancing)
Line monitoring	Line monitoring with LCP echo monitoring, dead-peer detection and up to 4 addresses for end-to-end monitoring with ICMP polling
VPN	
IPSec over HTTPS	Enables IPsec VPN based on TCP (at port 443 like HTTPS) which can go through firewalls in networks where e. g. port 500 for IKE is blocked. Suitable for client-to-site connections and site-to-site connections. IPSec over HTTPS is based on the NCP VPN Path Finder technology
Number of VPN tunnels	Max. number of concurrent active WireGuard or IPSec, PPTP (MPPE) and L2TPv2 tunnels: 5 (25 with VPN 25 Option). Unlimited configurable connections. Configuration of all remote sites via one configuration entry when using the RAS user template or Proadaptive VPN.
Hardware accelerator	Integrated hardware accelerator for 3DES/AES encryption and decryption
Realtime clock	Integrated, buffered realtime clock to save the date and time during power failure. Assures timely validation of certificates in any case
Random number generator	Generates real random numbers in hardware, e. g. for improved key generation for certificates immediately after switching-on
1-Click-VPN Client assistant	One click function in LANconfig to create VPN client connections, incl. automatic profile creation for the R&S®LANCOM Advanced VPN Client
1-Click-VPN Site-to-Site	Creation of VPN connections between R&S®LANCOM routers via drag and drop in LANconfig
IKE, IKEv2	IPSec key exchange with Preshared Key or certificate (RSA signature, ECDSA-Signature, digital signature)
Smart Certificate*	Convenient generation of digital X.509 certificates via an own certifaction authority (SCEP-CA) on the webpage or via SCEP.
Certificates	X.509 digital multi-level certificate support, compatible with Microsoft Server / Enterprise Server and OpenSSL. Secure Key Storage protects a private key (PKCS#12) from theft.
Certificate rollout	Automatic creation, rollout and renewal of certificates via SCEP (Simple Certificate Enrollment Protocol) per certificate hierarchy
Certificate revocation lists (CRL)	CRL retrieval via HTTP per certificate hierarchy
OCSP Client	Check X.509 certifications by using OCSP (Online Certificate Status Protocol) in real time as an alternative to CRLs
OCSP Server/Responder*	Offers validity information for certificates created with Smart Certificate via OCSP
XAUTH	XAUTH client for registering R&S®LANCOM routers and access points at XAUTH servers incl. IKE-config mode. XAUTH server enables clients to register via XAUTH at R&S®LANCOM routers. Connection of the XAUTH server to RADIUS servers provides the central authentication of VPN-access with user name and password. Authentication of VPN-client access via XAUTH and RADIUS connection additionally by OTP token

R&S®LANCOM IAP-5G

VPN	
RAS user template	Configuration of all VPN client connections in IKE ConfigMode via a single configuration entry
Proadaptive VPN	Automated configuration and dynamic creation of all necessary VPN and routing entries based on a default entry for site-to-site connections.
Algorithms	3DES (168 bit), AES-CBC and -GCM (128, 192 or 256 bit), RSA (1024-4096 bit), ECDSA (P-256-, P-384-, P-521-curves) and Chacha20-Poly 1305. OpenSSL implementation with FIPS-140 certified algorithms. MD-5, SHA-1, SHA-256, SHA-384 or SHA-512 hashes
Post-quantum security	Post-quantum Preshared Keys (PPK) for IKEv2
NAT-Traversal	NAT-Traversal (NAT-T) support for VPN over routes without VPN passthrough
MOBIKE	IKEv2 VPN clients can seamlessly switch between different networks (e.g. from WLAN to mobile radio) without having to re-establish the VPN tunnel
WireGuard	Support of WireGuard
R&S®LANCOM Dynamic VPN	Enables VPN connections from or to dynamic IP addresses. The IP address is communicated via the ICMP or UDP protocol in encrypted form. Dynamic dial-in for remote sites via connection template
Dynamic DNS	Enables the registration of IP addresses with a Dynamic DNS provider in the case that fixed IP addresses are not used for the VPN connection
Specific DNS forwarding	DNS forwarding according to DNS domain, e.g. internal names are translated by proprietary DNS servers in the VPN. External names are translated by Internet DNS servers
Split DNS	Allows the selective forwarding of traffic for IKEv2 depending on the addressed DNS domain.
IPv4 VPN	Connecting private IPv4 networks
IPv4 VPN over IPv6 WAN	Use of IPv4 VPN over IPv6 WAN connections
IPv6 VPN	Connecting private IPv6 networks
IPv6 VPN over IPv4 WAN	Use of IPv6 VPN over IPv4 WAN connections
Radius	RADIUS authorization and accounting, outsourcing of VPN configurations in external RADIUS server in IKEv2, RADIUS CoA (Change of Authorization)
High Scalability VPN (HSVPN)	Transmission of multiple, securely separated networks within a VPN tunnel
Advanced Mesh VPN	On demand dynamic VPN tunnel establishment between branches
IKEv2-EAP*	VPN clients can be authenticated with IKEv2-EAP against a central database like Microsoft Windows Server or RADIUS Server
Two-factor authentication*	Two-factor authentication with R&S®LANCOM Advanced VPN Client via IKEv2 EAP-OTP
***)**	Only with VPN 25 option
Performance	
Routing-Performance	Data regarding the overall routing performance can be found inside the R&S®NC tech paper "Routing-Performance" here.
VoIP	
SIP ALG	The SIP ALG (Application Layer Gateway) acts as a proxy for SIP communication. For SIP calls the ALG opens the necessary ports for the corresponding media packets. Automatic address translation (STUN is no longer needed).
Cellular radio	
Supported standards	5G, LTE, UMTS and HSPA support (mode of transmission automatically or manually adjustable), 2G/GSM is not supported
Supported 5G modes	5G standalone (SA), 5G non-standalone (NSA)
Supported mobile bands (5G)	n1 (2100 MHz), n2 (1900 MHz), n3 (1800 MHz), n5 (850 MHz), n7 (2600 MHz), n8 (900 MHz), n12 (700 MHz), n13 (700 MHz), n14 (700 MHz), n18 (850 MHz), n20 (800 MHz), n25 (1900 MHz), n26 (850 MHz), n28 (700 MHz), n29 (700 MHz), n30 (2300 MHz), n38 (2600 MHz), n40 (2300 MHz), n41 (2500 MHz), n48 (3500 MHz), n66 (2100 MHz), n70 (2000 MHz), n71 (600 MHz), n75 (1500 MHz), n76 (1500 MHz), n77 (3700 MHz), n78 (3500 MHz), n79 (4700 MHz)

R&S®LANCOM IAP-5G

Cellular radio	
Supported mobile bands (4G)	B1 (2100 MHz), B2 (1900 MHz), B3 (1800 MHz), B4 (1700 MHz), B5 (850 MHz), B7 (2600 MHz), B8 (900 MHz), B12 (700 MHz), B13 (700 MHz), B14 (700 MHz), B17 (700 MHz), B18 (850 MHz), B19 (850 MHz), B20 (800 MHz), B25 (1900 MHz), B26 (850 Mhz), B28 (700 MHz), B29 (700 MHz), B30 (2300 MHz), B32 (1500 MHz), B34 (2000 MHz), B38 (2600 MHz), B39 (1900 MHz), B40 (2300 MHz), B41 (2500 MHz), B42 (3500 MHz), B43 (3700 MHz), B48 (3500 MHz), B66 (1700 MHz), B71 (600 MHz)
Supported mobile bands (3G)	Band 1 (2100 MHz), Band 2 (1900 MHz), Band 4 (1700 MHz), Band 5 (850 MHz), Band 8 (900 MHz), Band 19 (800 MHz)
External antenna connectors	Four SMA antenna connectors (SMA female) for external mobile radio antennas
WWAN operating modes	Router or bridge mode
GPS	GPS positioning via enclosed antennas
Interfaces	
Ethernet ports	2 x 10/100/1000BASE-T full-duplex, autosensing (RJ-45), IEEE 802.3az, PoE (Power over Ethernet) at ETH1
Serial interface	Serial configuration interface / COM port (USB-C): 9,600 - 115,000 baud.
External antenna connectors	Four SMA antenna connectors for external 5G antennas
Hardware	
Power supply	Via Power over Ethernet, compliant with IEEE 802.3at
Environment	Temperature range -20°C to +50 °C; humidity up to 95%; non-condensing
Power consumption (Idle)	Approx. 5,6 W via power adapter (value refers to the power for the device and power adapter), about 7,8 W via PoE (value refers to the power for the device only)
Power consumption (max)	Approx. 11,3 W via power adapter (value refers to the overall power for thedevice and power adapter), about 13,2 W via PoE (value refers to the power for the device only)
Housing	Robust metal housing, IP 50 protection class, for wall, mast and top-hat rail mounting, 210 x 152 x 33 mm (length x width x depth)
Management and monitoring	
Management	R&S®LANCOM Management Cloud, LANconfig, WEBconfig, WLAN controller, R&S®LANCOM Layer 2 management (emergency management)
Management functions	Alternative boot configuration, voluntary automatic updates for LCMS and LCOS, individual access and function rights up to 16 administrators, RADIUS and RADSEC user management, remote access (WAN or (W)LAN, access rights (read/write) adjustable seperately), SSL, SSH, HTTPS, Telnet, TFTP, SNMP, HTTP, access rights via TACACS+, scripting, timed control of all parameters and actions through cron job
FirmSafe	Two stored firmware versions, incl. test mode for firmware updates
automatic firmware update	configurable automatic checking and installation of firmware updates
Monitoring	R&S®LANCOM Management Cloud, LANmonitor, WLANmonitor
Monitoring functions	Device SYSLOG, SNMPv1,v2c,v3 incl. SNMP-TRAPS, extensive LOG and TRACE options, PING and TRACEROUTE for checking connections, internal logging buffer for firewall events
Monitoring statistics	Extensive Ethernet, IP and DNS statistics; SYSLOG error counter, accounting information exportable via LANmonitor and SYSLOG
IPerf	IPerf is a tool for measurements of the bandwidth on IP networks (integrated client and server)
SLA-Monitor (ICMP)	Performance monitoring of connections
SD-LAN	SD-LAN – automatic LAN configuration via the R&S®LANCOM Management Cloud
SD-WAN	SD-WAN – automatic WAN configuration via the R&S®LANCOM Management Cloud
Hardware	
Weight	2,20 lbs (1,0 kg)

R&S®LANCOM IAP-5G

Declarations of conformity*	
CE	EN 62368, EN 55022, EN 55024
Country of Origin	Made in Germany
***) Note**	You will find all declarations of conformity in the products section of our website at www.rohde-schwarz.com/networks-and-cybersecurity
Scope of delivery	
Manual	Quick Installation Guide (DE/EN)
Cable	1 Ethernet cable, 3 m
Mounting Kit	Mounting kit for wall mounting
Antennas	Four 2 dBi 5G/LTE/UMTS-antennas
Power supply unit	External power adapter (230 V), NEST 12 V/2.0 A DC, coaxial power connector 2.1/5.5 mm, temperature range from -5 to +45° C, R&S®LANCOM item no. 111303 (EU)
Support	
Warranty extension	Free warranty extension up to 3 years (replacement service for defects) Find details here. The service and support conditions valid as of July 1, 2026, available at rs-nc.rohde-schwarz.com/fileadmin/pdf/LCS/ServiceSupportConditions/Rohde-Schwarz-Networks-and-Cybersecurity-GmbH-Service-and-Support-Conditions-20260701.pdf, apply.
Security updates	Up to 2 years after End of Sale of the device (but min. 3 years, see Link), can be extended by purchasing R&S®NC Support products
Software updates	Regular free updates including new features as part of the R&S®NC Lifecycle Management (Link)
Information on the EU Data Act	For details on product data and data on connected services, please refer to: Link
Manufacturer support	Available with R&S®NC products such as Support Access (for R&S®NC Community Partners only), Direct, or Premium
R&S®NC Support Access	Exclusively forR&S®NC Community partners: Personal manufacturer support (best effort) and security updates for the device, valid for all service categories, term-based (starting at the beginning of each quarter) for 1, 3, or 5 years (item no. 10804, 10805, or 10806)
R&S®NC Replacement Basic M	Security updates until EOL (min. 5 years) and 5 years replacement service with shipment of the replacement device within 5 days after arrival of the defective device (8/5/5Days), item no. 10721
R&S®NC Replacement Advanced M	Security updates until EOL (min. 5 years) and 5 years NBD advance replacement with delivery of the replacement device within one business day (8/5/NBD), item no. 10731
R&S®NC Support Direct 24/7 M	Direct, prioritized 10/5 manufacturer support incl. 24/7 emergency hotline and security updates for the device, guaranteed first response times (SLA) of max. 30 minutes for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years (item no. 10755, 10756 or 10757)
R&S®NC Support Direct Advanced 24/7 M	Direct, prioritized 10/5 manufacturer support incl. 24/7 emergency hotline and security updates for the device, NBD advance replacement with delivery of the device on the next business day (24/7/NBD), guaranteed first response times (SLA) of max. 30 minutes for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years (item no. 10779, 10780 or 10781)
R&S®NC Support Direct 10/5 M	Direct, prioritized 10/5 manufacturer support and security updates for the device, guaranteed first response times (SLA) of max. 2 hours for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years.(item no. 10743, 10744 or 10745)
R&S®NC Support Direct Advanced 10/5 M	Direct, prioritized 10/5 manufacturer support and security updates for the device, NBD advance replacement with delivery of the device on the next business day (10/5/NBD), guaranteed first response times (SLA) of max. 2 hours for reporting massive operational disruptions by telephone (priority 1) and max. 4 hours for all other concerns (priority 2), term-based for 1, 3, or 5 years.(item no. 10767, 10768 or 10769)
Software	
Lifecycle Management	After discontinuation (End of Sale), the device is subject to the R&S®NC Lifecycle Management. Details can be found at: Link

LCOS 10.94

R&S®LANCOM IAP-5G

Software	
IT Security made in Germany	The development and quality assurance take place in Germany in accordance with high security standards. The „IT Security made in Germany" quality label of the German IT Security Association attests to the level of security achieved.
Options	
VPN	R&S®LANCOM VPN-25 Option (25 channels), item no. 60083
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 1-Year (for R&S®LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller R&S®LANCOM WLC-60), item no. 62168
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 3-Years (for R&S®LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller R&S®LANCOM WLC-60), item no. 62169
R&S®LANCOM Security Essentials	R&S®LANCOM Security Essentials B Option 5-Years (for R&S®LANCOM SD-WAN gateways of the 700, 800, 1600, 1700, 1800, IAP, and OAP series as well as WLAN controller R&S®LANCOM WLC-60), item no. 62170
R&S®LANCOM BPjM Filter	R&S®LANCOM BPjM Filter Option, 5 years subscription, item no. 61418
R&S®LANCOM Public Spot	Hotspot option for R&S®LANCOM products, versatile access (via voucher, e-mail, SMS), including a comfortable setup wizard, secure separation of guest access and internal network, item no. 60642
R&S®LANCOM Public Spot (10 bulk)	Hotspot option for R&S®LANCOM products, versatile access (via voucher, e-mail, SMS), including a comfortable setup wizard, secure separation of guest access and internal network (10 bulk), item no. 61312
R&S®LANCOM Management Cloud	
R&S®LANCOM Management Cloud	R&S®LMC-B-1Y License (1 Year), enables the management of one category B device for one year via the R&S®LANCOM Management Cloud, item no. 50103
R&S®LANCOM Management Cloud	R&S®LMC-B-3Y License (3 Years), enables the management of one category B device for three years via the R&S®LANCOM Management Cloud, item no. 50104
R&S®LANCOM Management Cloud	R&S®LMC-B-5Y License (5 Years), enables the management of one category B device for five years via the R&S®LANCOM Management Cloud, item no. 50105
Accessories	
External antenna	R&S®AirLancer O-360Q-5G, omnidirectional outdoor antenna MIMO (4x4), for all 4G/5G bands (700-3800 MHz), item no. 61234
Surge arrestor (LAN cable)	R&S®AirLancer SN-LAN surge arrestor (LAN cable), item no. 61261
R&S®LANCOM IAP Mount	R&S®LANCOM IAP Mount for cap rail and pole mounting, item no. 61647
R&S®LANCOM PoE++ Injector (EU)	1-port PoE injector with multi-Gigabit support, integrated power supply, compatible with the standard IEEE 802.3af/at/bt (up to 65W), item no. 61779 (EU)
VPN Client Software	R&S®LANCOM Advanced VPN Client for Windows - single license, item no. 61600
VPN Client Software	R&S®LANCOM Advanced VPN Client for Windows - 10 licenses, item no. 61601
VPN Client Software	R&S®LANCOM Advanced VPN Client for Windows - 25 licenses, item no. 61602
VPN Client Software	R&S®LANCOM Advanced VPN Client for Mac OS X, single license, item no. 61606
VPN Client Software	R&S®LANCOM Advanced VPN Client for Mac OS X, 10 licenses, item no. 61607
Item number(s)	
R&S®LANCOM IAP-5G	61718

Rohde & Schwarz Networks and Cybersecurity GmbH
Adenauerstr. 20/B2
52146 Wuerselen | Germany
info.rs-nc@rohde-schwarz.com | www.rohde-schwarz.com/networks-and-cybersecurity

R&S and Rohde & Schwarz are trademarks of Rohde & Schwarz GmbH & Co. KG, registered or used, among others, in Germany, the EU, the USA, China, and other countries. Other names or designations used may be registered trademarks of different companies or owners. This document contains forward-looking statements regarding products and product features. The publisher reserves the right to change these at any time without stating reasons. No liability is accepted for technical inaccuracies or omissions. 09/2026