

Service certificate

STACKIT VPN

**Version and start of
validity**

Version 1.0	Valid from 05.05.2026
-------------	-----------------------

Service certificate | STACKIT VPN

Service name

STACKIT VPN

High level service description

The **STACKIT VPN** product enables customers to provide secure, scalable and flexible virtual private network connections (VPN) in the STACKIT cloud environment. With STACKIT VPN, customers can connect their on-premises data centers or their office locations to their STACKIT cloud resources to ensure encrypted data transmission and robust network security. The Customer can choose between different VPN configurations, including site-to-site, site-to-multisite, and active-active connections to meet the specific needs of their company. The provision, administration and configuration of the VPN is carried out by the Customer via the STACKIT API as well as the STACKIT Portal or the STACKIT Developer Tools..

Key features

- **Flexible VPN configurations:** Support for different VPN types including site-to-site, site-to-multisite and active-active VPNs to cover different use cases and business requirements..
- **Secure data transmission:** End-to-end encryption of all data transmitted via the VPN to ensure the highest security standards.
- **High availability:** Ability to implement redundant VPN connections and active-active setups to maximize reliability and minimize downtime.
- **Self-service provisioning:** Administration, configuration and monitoring of the VPN via the STACKIT API or the STACKIT portal.
- **Scalability:** Dynamic adaptation of VPN connections according to growing demand without the need for extensive infrastructure changes.

Service plans

The Customer has the option of selecting from various configurations of the service as part of the order. These differ primarily in their maximum bandwidth and number of possible connections.

Metric

- **Billing:** Per VPN gateway per started hour according to the selected service plan.
- **Calculated period:** Creation of the VPN gateway until deletion of the corresponding resource.

- For additional resources used by the Customer in connection with STACKIT VPN, such as STACKIT Observability, a separate calculation is made according to the conditions specified in the respective service specifications.

SLA specifics

The STACKIT VPN service offering is subject to the general SLA provisions as defined in the [STACKIT Service Description](#). Additional, specific service level agreements for STACKIT VPN are listed below:

- The SLA only applies to VPN gateways that are configured in Active-Active mode. It is the responsibility of the Customer to redundantly connect and configure both instances provided in the VPN gateway (tunnel 1 and tunnel 2) on their local gateway (customer gateway).
- A VPN connection is considered available if at least one of the two STACKIT VPN gateway instances is operational and can process traffic via an established tunnel.
- The connection is considered unavailable if both instances of the STACKIT VPN gateway cannot establish external connectivity at the same time and this is due to the STACKIT infrastructure. This is the case if:
 - Neither of the two STACKIT VPN instances can be reached via the public network.
 - STACKIT errors prevent the setup of both tunnels despite correct customer configuration..

Backup

Backup and recovery of the VPN configurations and data are the responsibility of the Customer and are not included in the service. This relates in particular to:

- The configuration of the VPN gateway and VPN connections, including all characteristics and settings specified by the Customer.
- The log data and connection information that is generated in connection with the use of the VPN service.
- Securing access data and certificates used for authentication and encryption of VPN connections.

Additional terms

- The VPN settings and connections configured by the Customer are not part of the service scope of STACKIT VPN and are the sole responsibility of the Customer.
- The Customer is responsible for the management of the VPN configurations, including the management of access data and certificates. This includes, in particular, the creation, maintenance, updating and securing of the VPN settings.
- STACKIT provides support for technical issues related to the VPN infrastructure itself, but not for the specific configuration or operation of the VPN on the Customer side.
- The Customer bears the responsibility for the security of their VPN connections and compliance with applicable security policies. In particular, this includes ensuring that there is no unauthorized access to the VPN or the data transmitted via the VPN.

STACKIT provides the relevant security measures of the VPN infrastructure in accordance with the requirements of §§ 165 ff TKG.

- The current information on supported VPN protocols, encryption standards and configuration options are available in the [STACKIT knowledgebase](#). STACKIT reserves the right to change or expand the offered VPN functions and configurations. Changes will be updated accordingly in the documentation. Material changes will be communicated to the Customer at least one month before they become effective via the STACKIT release notes; § 57 TKG remains unaffected.
- The Customer undertakes to comply with all legal requirements and regulatory requirements in connection with the use of the VPN service for the purposes of the Customer. STACKIT fulfills the regulatory obligations applicable on a telecommunications service provider (in particular under the TKG and the TDDDG).
- The Customer is obliged to carry out regular security checks and to ensure the integrity of the VPN connections.

Annex | Exportability

(Online Register)

Data type	Description	Exportable (Yes/No)	Format	Additional notes
Customer data (database content)	VPN gateway & VPN connection configuration data	Yes	JSON	All configurations created by the Customer, apart from passwords (PSK), can be exported via the STACKIT VPN API or viewed via STACKIT Portal.
	Connection data	No	-	For a VPN service, the primary 'data content' is the traffic being passed through. This traffic is not stored.
User accounts & permissions	Information about users and their permissions	No	-	The STACKIT VPN service does not store any accounts or permissions. Auth happens entirely via STACKIT IAM.
System metrics (instances / resources in use)	Performance data of the instance / resource in use (e.g., CPU usage, memory usage)	Yes	JSON	Contains data such as number of active connections and data volume. Values can be queried via the STACKIT VPN API or viewed in the STACKIT portal. The Customer can (in the future, optional) configure his own observability instance to which this and other performance data of the VPN instances can be sent. This instance is under the control of the Customer.
	Sizes and capacities	Yes	JSON	These are the contractually agreed or booked service limits, e.g. B. Maximum bandwidth, maximum permitted number of connections or the number of booked VPN gateways.
	Capacities of the available resources / instances			Values result from the VPN plan and project quotas booked by the Customer and can be viewed via the STACKIT VPN API or in the STACKIT portal.

System properties (instances / resources in use)	Versions and information necessary to check compatibility	Yes	JSON	The data can be viewed in the STACKIT portal and via the STACKIT VPN API, e.g. currently created VPN gateways & connections as well as encryption algorithms and authentication methods. VPN protocols, encryption algorithms and authentication methods supported by STACKIT VPN can be viewed in the STACKIT documentation, the STACKIT portal and STACKIT VPN API docs.
Product / service-related data (product properties)	Configuration data and source code	No. Company confidential STACKIT		
	<i>Configuration of IT-systems / rudimentary IT, settings, customizing, IP's, VLAN, interfaces, software code, scripts</i>			
	Log data (non personalized and personalized)	Yes	-	The Customer can (in the future, optional) configure his own observability instance to which the log data of the VPN connections (connection establishment, termination, status) of the VPN instances can be sent. This instance is under the control of the Customer.
	<i>System-status, technical-events, etc.</i>			
	Log data (non personalized and personalized)	Yes	JSON	All API-Calls to STACKIT VPN API via STACKIT Telemetry Router.
	<i>Login/logout of user, user activities</i>			