Rohde & Schwarz Cybersecurity

R&S®TRUSTED VPN CLIENT

In case you need to access a government agency network securely on the go: R&S®Trusted VPN Client protects organizations’ internal network communications between the client platform and the VPN gateway. Start connecting laptops and notebooks to the Intranet in a secure manner, even when data traffic is routed over the Internet.

The solution is purely software based thanks to the cutting-edge architecture of the R&S®Trusted VPN Client. It even meets the high security level with RESTRICTED classification level approval. End users access the standard Microsoft® Windows 10™ platform, while administrators manage the easy-to-install software package on the existing system.
R&S®Trusted VPN Client – application scenarios

► Work from anywhere
Employees can easily leverage the advantages of virtual workstations when traveling or working from home. They get a hold of confidential data securely over the internet, including emails, documents, VoIP calls or the organization’s Intranet. Access is possible using a LAN connection or mobile connections such as Wi-Fi. Wi-Fi hotspots using login mechanisms (captive portals) are also supported.

► On-the-go connections
The R&S®Trusted VPN Client automatically logs into already known networks and establishes a VPN connection. This enables employees to work on the go without any restrictions. They stay connected to the Intranet, even when switching between different wireless networks.

► Data loss prevention
It is not possible to bypass the R&S®Trusted VPN Client. Therefore, access to the organization’s network without using a secure VPN connection is not possible.

► Remote maintenance
By using a secure channel, organizations’ internal IT administrators can even remotely configure and troubleshoot the R&S®Trusted VPN Client on endpoint devices.

R&S®Trusted VPN Client – advantages

Protection via BSI-compliant cryptographic methods
The cryptographic methods and security mechanisms comply with the RESTRICTED requirements of the German Federal Office for Information Security (BSI).

Flexible, software based use
The VPN client is fully software based and supports conventional hardware requirements. Establishing a VPN connection does not require the use of third-party devices.

Easy administration for secure remote connections
Existing VPN gateways from different manufacturers are supported. Optionally, the R&S®Trusted VPN gateway can be used. It is possible to integrate existing public key infrastructures (PKI). For the rollout of internal installations and updates, organizations and companies simply use existing software deployment systems. IT administration is also straightforward thanks to the R&S®Trusted Objects Manager.

Multi-factor authentication
Secure access authorization is provided by several independent authentication mechanisms such as PIN and smartcard, for example as part of a badge or ID card.

R&S®Trusted Endpoint Suite
The R&S®Trusted VPN Client is embedded in the R&S®Trusted Endpoint Suite. This combined modular security solution ensures comprehensive system protection within government agency or company networks.

Additional components such as the:
► R&S®Trusted Disk
  for full disk encryption
► R&S®Browser in the Box
  for secure Internet surfing
  can be used and configured individually to meet customer requirements.