

ANDROID VPN CLIENT

The trusted VPN client for your mobile connections

The Android VPN Client secures data exchanges to and from smartphones and tablets. While it is particularly suitable for managing industrial systems (maintenance, diagnostics, logistics, etc.), it also meets the requirements for protecting critical communications of public and private security services.



High level security

The Android VPN Client has been developed according to recommendations from NIST and ANSSI. The protocols in the current version meet the IPsec DR profile for restricted communications. The software is thus compatible with the ANSSI's IPsec Restricted framework.

The many protocols and algorithms implemented in the software make it a universal client allowing your users to connect to any OpenVPN or IPsec VPN firewall/gateway on the market, regardless of whether it is software or hardware-based, including those that support the IPsec Restricted repository.



Easy to install

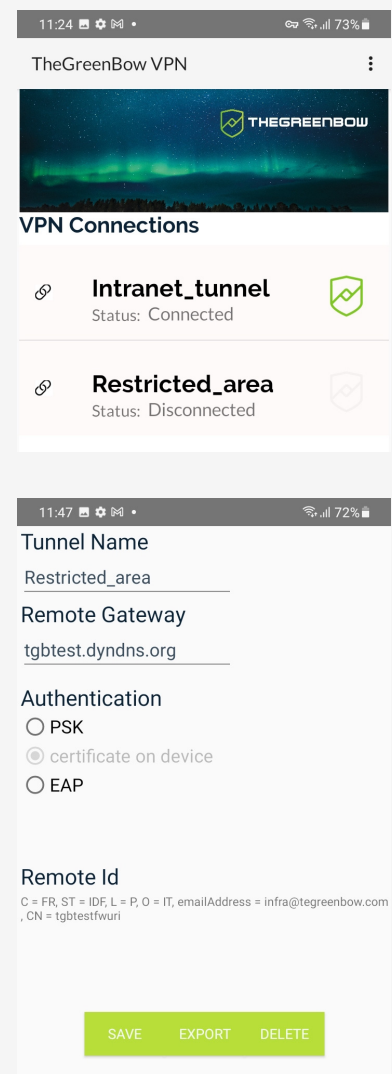
Installation on any terminal running Android is entirely transparent for users. The software supports a variety of protocols, settings, and options that enable interoperability with your gateway/firewall and your PKI. The Android VPN Client is now able to access certificates stored in the Android certificate store, which makes installation even easier.



Simple to use

The Android VPN Client makes it easy to use a VPN, owing to its user-friendly interface that helps your users establish secure connections to your information system.

Users get a direct view of the status of their VPN connections to ensure that their communications are properly protected. They can also rely on the Always-on VPN feature for peace of mind, knowing that their device will remain protected in any situation with no action required from them.



TECHNICAL DATA

Protocols	<ul style="list-style-type: none"> ● IPsec IKEv2 ● OpenVPN ● Network: IPv4, NAT-Traversal, IKE fragmentation
Authentication	<ul style="list-style-type: none"> ● EAP, PSK, certificates, Extra Auth, Multiple Auth ● X.509 certificate management: PKCS#12, PFX
Cryptography	<ul style="list-style-type: none"> ● DH 14-21 & 28, AES 128/192/256 SHA-2 (256/384/512) ● Certificate authentication methods: Method 1: RSA Digital Signature with SHA-2 [RFC 7296] Methods 9-11: ECDSA “secp” with SHA-2 [RFC 4754] Method 14: RSASSA-PKCS1-v1_5, RSASSA-PSS [RFC 7427] Method 214: ECDSA “BrainpoolP256r1” with SHA-2
System requirements	<ul style="list-style-type: none"> ● Android 10 or higher ● 40 MB of available disk space for the app and data

Main features

- Compatible with gateways that support the IPsec Restricted repository
- Import certificates from the Android certificate store
- Keep VPN always on, even when the client is not running
- Activate licenses using TAS (manually or within a tunnel)
- New graphical interface
- Check gateway CAs
- Tunnel management: full tunneling, split tunneling
- Service continuity: Dead Peer Detection (DPD), redundant gateway
- Automatically retrieve network parameters from gateway (CP mode)
- Configure and establish SSL connections (OpenVPN)
- End of support for IKEv1

