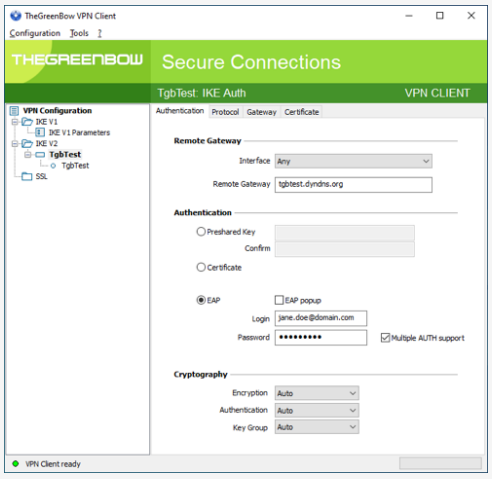
WINDOWS STANDARD VPN CLIENT

The trusted VPN client for your remote connections

The Windows Standard VPN Client is easy to install and use in an existing infrastructure, making it a suitable choice for information systems in very small to medium-sized businesses. Digital nomads and teleworkers can rest assured that their requirements for secure communications are met.

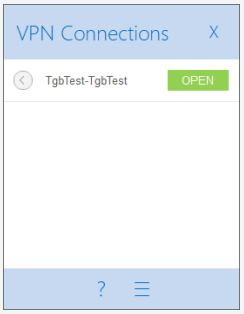
High level security

The Windows Standard VPN Client has been developed according to recommendations from NIST and ANSSI. It accounts for available authentication functions in the information system, and thus is compatible with most existing PKIs. 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.



Easy to install

The software features a wizard that guides you through installation on any Windows 10 workstation in but a few mouse clicks. It offers a variety of protocols, settings, and options that ensure interoperability with your equipment.
A configuration wizard guides you through the setup of your VPN connections for easy integration with your firewall or gateway.



Simple to use

The Windows Standard 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. A full-featured administration interface provides access to all the settings required to define the security rules to be applied to the workstation.

TECHNICAL DATA

Protocols	• IPsec: IKEv1, IKEv2 • OpenVPN • Network: IPv4, IPv6, NAT-Traversal, IKE fragmentation
Authentication	• Strong user authentication: EAP, X-Auth, PSK, tokens and smart cards • X.509 certificate management: DER/PEM; PFX/P12
Cryptography	• DH 14-21, AES-CBC, AES-GCM, AES-CTR (128/196/256), SHA-2 (256/384/512) • Extended Sequence Number [RFC 4304] and Childless IKE Initiation [RFC 6023] • Support for Microsoft CNG (Cryptography API: Next Generation) and PKCS#11 APIs for tokens and smart cards • Certificate authentication methods: Method 1: RSA Digital Signature with SHA-2 [RFC7296] Method 9: ECDSA "secp256r1" with SHA-256 on the P-256 curve [RFC4754] Method 10: ECDSA "secp384r1" with SHA-384 on the P-384 curve [RCF4754] Method 11: ECDSA "secp521r1" with SHA-521 on the P-521 curve [RCF4754] Method 14: Digital Signature Authentication PKCS1-v1.5 [RCF7427]
System requirements	• Windows 10, Windows 11, 64-bit • Intel 1 GHz processor • RAM: 2 GB • 40 MB of available disk space

Main features

- Installation and configuration wizard
- Support for tokens and smart cards
- Tunnel management: full tunneling, split tunneling, multiple simultaneous tunnels
- Connect automatically: as soon as traffic is detected, or when a USB stick, token, or smart card is inserted
- Execute scripts when opening/closing a connection
- Service continuity: Dead Peer Detection (DPD), redundant gateway, fallback tunnel
- Credential Providers mode (starts before Windows logon)

THEGREENBOW

TheGreenBow – 14 rue Auber, 75009 Paris, France – sales@thegreenbow.com – +33 1 43 12 39 37
https://www.thegreenbow.com