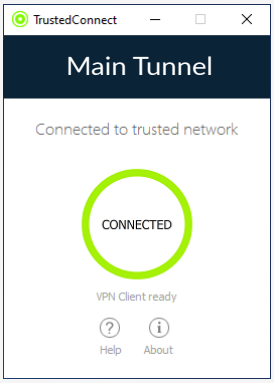
WINDOWS ENTERPRISE VPN CLIENT 7

The trusted VPN client for all organizations

The Windows Enterprise VPN Client is a lasting solution for complex or extensive information systems, as it is easy to deploy and integrate into any existing infrastructure. An independent auditing body has certified that our software meets the requirements for securing the communications of major organizations, critical market operators, operators of essential services, and public administrations.

High level security

The Windows Enterprise VPN Client has been developed according to recommendations from NIST and ANSSI. It accounts for available authentication functions in the information system, and thus includes mechanisms to integrate with existing PKIs. All the protocols and algorithms implemented in the software make it a universal client allowing you to connect to any VPN gateway on the market, regardless of whether it is a software or a hardware, including those that support the IPsec Restricted repository.



Easy to install

Using the capabilities that come with the Windows installer (MSI), administrators benefit from fleet management tools and user groups (GPOs) to deploy and administer the Windows Enterprise VPN Client. In addition to silent installation, scripts, numerous customization and pre-configuration options, such as user interface customization, PKI functions can be configured in a fully centralized manner.

Simple to use

Protecting your users' connections requires that you make it easy for them to adopt a VPN. This is why we have made using the Windows Enterprise VPN Client as simple as possible with three different modes. The simplest of the three is the "Always-On" mode. We have stripped its interface to the bare essentials, and named it TrustedConnect. It detects and clearly shows whether the user is connected to a trusted network. If this is not the case, it automatically establishes a secure tunnel, seamlessly switching between Wi-Fi, 4G/5G, or a wired network. The standard mode simply enables users to activate any available tunnels. They can then access the various resources they need on the remote network. Administrators get access to the full interface with all the settings, e.g. to define the security rules to be deployed on the organization's workstations.

TECHNICAL DATA	
Protocols	• IPsec: IKEv2 • OpenVPN • Network: IPv4, IPv6, NAT-Traversal, IKE fragmentation
Authentication	• Automatic certificate detection on all media • Strong user authentication: EAP, X-Auth, PSK, smart cards, tokens, PKCS#11 • X.509 certificate management: DER/PEM; PFX/P12
Cryptography	• DH 14-21 & 28, AES-CBC, AES-GCM, AES-CTR (128/192/256), SHA-2 (224/256/384/512) • Support for RFC 4304 Extended Sequence Numbers (ESNs) and RFC 6023 (Childless IKE Initiation) • Support for the Microsoft Cryptography API: Next Generation (CNG API) • Authentication methods: 1, 9, 10, 11, 14, 214 (RFC 4754, 7296, 7427)
System requirements	• Windows 10, Windows 11, 64-bit • 1 GHz x86-64 processor • RAM: 2 GB • 40 MB available disk space

Main features

- Compatible with gateways that support the IPsec Restricted repository
- Filtering mode, Captive Portal Detection (CPD), and Always-On mode
- Trusted Network Detection (TND) using HTML beacons or Active Directory (AD)
- Automatic tunnel opening: when traffic is detected, on token or smart card insertion
- Credential Providers mode (start tunnel before Windows logon)
- Dedicated configuration interface for administrators
- System and administrator logs
- Service continuity: Dead Peer Detection (DPD), redundant gateway, fallback tunnel
- Advanced deployment features: silent installation and updates, customization, scripts
- Advanced tunnel management: all through the tunnel, tunnel within the tunnel, multiple simultaneous tunnels, disable split tunneling

THEGREENBOW

TheGreenBow – 28 rue Caumartin, 75009 Paris, France – sales@thegreenbow.com – +33 1 43 12 39 37
www.thegreenbow.com