[Product Spotlight] TheGreenBow: More Than a VPN

WE ARE PLEASED TO TAKE A CLOSER LOOK AT THE LEADING VPN SOLUTION

Occasionally, we shine the spotlight on a third-party product that we find impressive and want to share with our community. Today, we are pleased to take a closer look at the leading VPN solution, TheGreenBow.

About TheGreenBow

TheGreenBow is one of the world's most trusted VPN software publishers. The company has more than two million users in over 70 countries, and they serve small and mid-sized businesses, mid-market organizations, large enterprises, and major corporations, including critical market operators, public administrations, and local authorities.

Since launching in 1998, TheGreenBow has helped its customers manage privacy, governance, and security issues at the highest level. They are the first European VPN software provider to obtain the EAL3+ Common Criteria certification, as well as NATO and EU Restricted approval for their Windows VPN Client. They have also earned the "As Used by the French Armed Forces" designation, which certifies that the French Ministry of Armed Forces has implemented their software. A 30-day free trial is available. Learn more at: https://www.thegreenbow.com/en/products/thegreenbow-vpn-clients-download/

TheGreenBow's Key Features

TheGreenBow offers several key features that set its VPN apart from many other VPN solutions on the market. Here are some aspects that the team here at Devolutions has found particularly impressive:

Multiple Clients

TheGreenBow supports multiple clients, including: Windows Standard, Windows Enterprise, Windows Enterprise Certified, macOS, iOS, Linux, Linux Certified, Android, and TheGreenBow Activation Server. Clients are compatible with all gateways, and they align with IPSEC IKE V2 protocols.

Strong and Flexible Authentication

Users can choose from various strong authentication options, including: certificates, tokens, and smart cards. The certificate is unique to each user, has a fixed duration, and can be revoked in the event of a cyberattack or other issue. For even more security, a second layer of authentication is available via a double tunnel (more on this below).

Intuitive User Experience

Although TheGreenBow is a powerful VPN, getting set up is surprisingly fast and easy. The installation is handled by an MSI installer package, the product integrates with Azure AD, and everything is monitored through a dashboard and feature called the TrustedConnect Panel (this is explored further in this article). Speaking of the interface: Various modules can be hidden from the taskbar menu as desired (e.g., console, connection panel, configuration panel, etc.). It is also possible to hide the pop-up window that appears when a tunnel is opened or closed. TheGreenBow's ease-of-use is a major benefit vs. several other VPNs that are excessively complicated to configure, and which often require a level of IT expertise that many smaller organizations do not have in-house.

Nested Tunnels

Earlier, we noted that users can create double tunnels to add a second layer of security. A really nice feature here is that the tunnels are nested, which means that when the first tunnel is closed the second one automatically closes at the same time.

Dead Peer Detection

One of the biggest reasons end users dislike VPNs (and some of the more tech savvy among them try to circumvent it) is that they have to deal with service interruptions — which means they cannot get their work done. TheGreenBow has built-in dead peer detection (DPD), which automatically activates when a tunnel is open. When linked to a redundant gateway, DPD enables the VPN client to automatically switch between gateways when one of them is unavailable — thereby allowing continuity of service. The redundant gateway can be different or identical to the main one (which means that organizations can benefit from the automatic reopening mode without having to use two gateways).

Automation

The Windows Standard VPN client can perform automated actions for each VPN tunnel, such as switching to a fallback tunnel, opening the tunnel automatically if certain criteria are met, running batches or scripts at various stages while opening or closing a tunnel, etc. Also, opening a tunnel can be customized to automatically run a specific script.

GINA Mode

TheGreenBow's GINA mode (available in the Windows Enterprise VPN client) allows organizations to open VPN connections before the Windows logon. This is ideal for creating a secure connection to an access rights management server, so that user workstation access rights can be obtained before opening a user session.

Remote Desktop Sharing

Typically, opening a remote desktop session over the internet requires establishing a secure connection and entering the connection parameters (address of the remote computer, etc.). This can be time-consuming, and creates the possibility of input error. TheGreenBow simplifies this process. With a single click, it establishes a VPN connection to the remote workstation, and then automatically opens a Remote Desktop Protocol (RDP) session.

TrustedConnect Panel

An especially impressive feature in TheGreenBow VPN is the TrustedConnect Panel (available in the Windows Enterprise client). The TrustedConnect Panel allows users to permanently maintain a secure connection to a trusted network. There are two components:

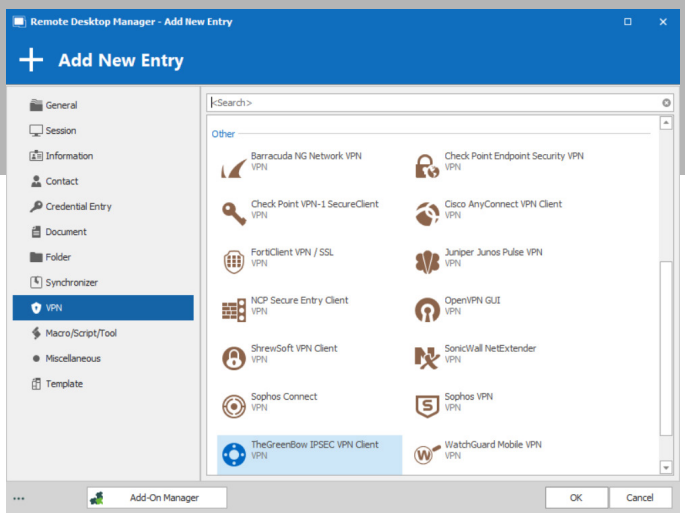
- Trusted Network Detect (TND) determines whether the workstation is inside a trusted network based on DNS suffixes and beacon identification.
- Always-On ensures connection security is maintained during each network interface change (e.g., between Ethernet, Wi-Fi, and 4G/5G). What's more, the icon in the taskbar and the connection status indicator ring are color-coded based on the current status of the TrustedConnect Panel:
- Blue: The workstation is directly connected to the company's trusted network (Administrators have the option to disable this color, in which case this status will be displayed in green).
- Green: The workstation is connected to the corporate network via a VPN connection, which means that it is physically on an untrusted network.

Integration with Remote Desktop Manager

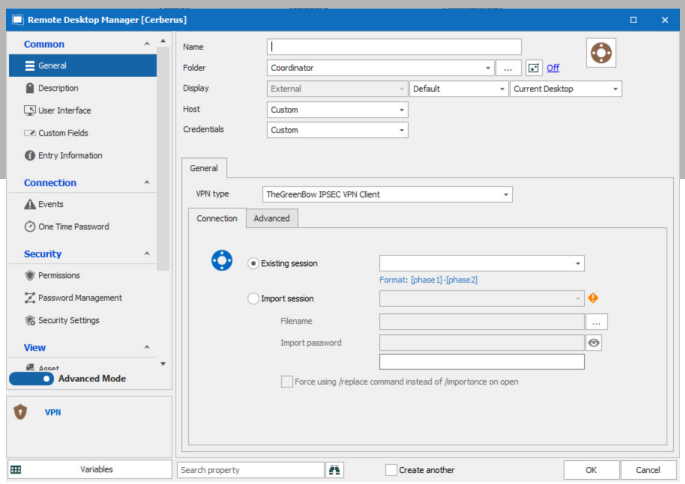
We are also pleased to note that TheGreenBow is integrated into Remote Desktop Manager. The configuration is pretty easy:

- For a new entry, follow these simple steps:

1. Click on **Add New Entry**, then select the VPN you want to work with. Here, it's **TheGreenBow IPSEC VPN Client**.



2. Set up your entry and your VPN options.



3. Run your session when everything is set up.

Link it to an existing session

To find out how to configure a VPN using TheGreenBow with an existing session, please refer to this walk-through, which includes screenshots: https://kb.devolutions.net/rdm_how_configure_vpn_existing_session.html

Launch a Free Trial

If you would like to give TheGreenBow a test run, a free trial of TheGreenBow VPN is available here: https://www.thegreenbow.com/en/products/thegreenbow-vpn-clients-download/