VPN Dialer Pro & Enterprise
Product Information

Table of Contents

Product Description

VPN Dialer is software-only persistent VPN connectivity solution that leverages dial-up VPN technology already built into Windows operating systems. Once installed and configured, it operates without a user interface, to automatically maintain a “nailed-up” or persistent VPN connection in the background, for as long as the computer has power and Internet access available to it. It will make this connection in the background even before anyone has logged into the desktop.

You can use VPN Dialer to design a persistent VPN infrastructure that is totally self-contained and does not rely on a third party to transfer data – your company’s workstations are simply and persistently connected directly to your company’s VPN server(s) and stay connected.

Advanced features of VPN Dialer include: the ability to specify additional routers on the local subnet, performance optimization through the automatic PING testing for the fastest path when multiple

routers and/or VPN servers are configured, automatic rejection of an IP address if it is not consistent with the expected static IP address (allowing for a reconnection, until the expected IP address is assigned), and automatic detection of a stale VPN connection and performing an automatic disconnect and reconnect.

There are many competing VPN technologies in the marketplace. VPN Dialer is most suitable for deployment scenarios where a company wants to have a self-contained persistent VPN infrastructure covering geographically dispersed Windows-based laptops and desktop computers, without relying on specialized VPN hardware, while using standard VPN standards and technologies, and without having to trust or relay sensitive company data through a third party network.

The best way to verify VPN Dialer is the best solution for your usage scenario is to download and install the free 30-day trial version of VPN Dialer at https://www.vpndialer.com . The functionality difference between the trial version and Pro and Enterprise have to do with activation and expiration, and you can fully validate the suitability of VPN Dialer using the trial version.

Comparison: Free Trial vs. Pro vs. Enterprise

	Free Trial	Professional	Enterprise
Support Period	N/A	One or Three Years	Three Years
VPN Servers Supported	Up to 3	Up to 3	Up to 3
Licensing	Free for 30 days Acts like a subscription limited to 30 days	$40 1-Year Subscription $97 Permanent w/1YR $127 Permanent w/3YR Above are per computer.	$14,995 per enterprise; VPN Dialer may be installed on an unlimited number of computers and activated, for the designated corporate servers.
Workstation Feature Set	Fully functional for the entire 30-day trial period.	Fully functional for the licensed workstation for one year, or in perpetuity, depending on the license. The support period is one or three years depending on the variety purchased.	Fully functional for all computers in the enterprise installed and activated during the support period, which once installed functional in perpetuity. The support period included with original purchase is three years.
Enterprise Feature Set	Fully automated client installation script support.	Fully automated client installation script support.	Fully automated client installation script support. Special command line utilities to list, add, and delete Windows RRAS

			VPN accounts.
Renewal	Free for 30 days, supports in-place upgrade by purchasing a Pro or Enterprise license key.	Subscription may be extended by purchasing additional license keys at $40 each. VPN Dialer Pro perpetual license support may be extended for $40 per *two* years.	The support period may be extended for $3,495 per year, after the first three years.

Comparison of VPN Technologies

There are many VPN technologies, and it can be confusing trying to sort them out. This document describes them and shows their similarities and differences.

SSL VPN

Examples. Some popular SSL VPN products include hardware from SonicWALL*, Cisco*, and Juniper*; and software-based SSL VPN products from VPN Labs*, and OvisGate*.

Explanation. The basic idea of an SSL VPN is to provide an interface over a web browser, to give remote users access to company resources such as documents and applications, but in a strictly controlled and limited fashion. Its benefit is mainly in security, as it effectively controls what remote users may do when accessing the company network from a remote location. Some disadvantages include the fact this is a remote access portal which must be configured, and does not work in the same way accessing resources on the local network does. This involves some configuration and training overhead.

Similarities and Relationships. SSL VPNs can be thought of as being more of a "portal" technology to make specific applications and data available to remote users, than a "VPN" technology that makes the entire network available. That is not to deny its usefulness, but keeping this in mind help avoid confusion.

Dial-Up VPN (Often Implemented with PPTP, L2TP/IPSec, IPSec, and SSTP)

Examples. Examples of dial-up VPN clients include the built-in VPN RAS client in Microsoft* Windows*, Cisco* VPN Client, and PPTP and L2TP/IPSec clients available for Linux.

Description. Dial-up VPN is a successor technology to simple dial-up network access using a modem, over a regular telephone line – such as dial-up Internet connection so common in the early days of the Internet. Rather than "dialing" a telephone call with a modem, dial-up VPN makes an encrypted tunnel connection through an Internet connection that is already available, to a remote network. Information can be exchanged with the remote network with security, as the information is encrypted. In practice, making a dial-up VPN connection causes the connecting computer to temporarily become a part of the remote network, for the duration of the connection. The benefit to this type of VPN is that it provides the mobile professionals and telecommuters with access to the company network in much the same way the network is accessed while physically being there.

Similarities and Relationships. Dial-up VPN is like and a successor technology to modem dial-up network access. This technology forms the foundation upon which Site-to-Site VPN technology is built. It also forms the basis for Persistent Dial-Up VPN technology.

Site-to-Site VPN (Often Implemented with IPSec)

Examples. Some commonly used Site-to-Site VPN products include Windows* Server 2003 RRAS configured to connect multiple locations, inexpensive Linksys*, DLink*, Netgear* IPSec VPN routers which can be configured to connect to each other, and advanced Cisco* and other premium VPN routers that support configurations with redundant paths and aggregation of data over multiple links.

Explanation. The basic idea of site-to-site VPN is to make a permanent connection between multiple sites (such as the main company network, and each branch office), so all systems in the company can communicate with each other as if they are on the same large network. One significant benefit for administration, is that you can access remote systems physically located in a different location, from the moment it boots up, because the site-to-site VPN server or device keeps the networks connected regardless of individual devices being logged in or not. This means you can also access printers and other network devices company-wide. Devices and computers do not need any VPN software to be part of the company-wide network. Site-to-Site VPN often builds on Dial-Up VPN technology, with dedicate devices performing the function of maintaining a permanent connection, and routing information between networks.

Advanced Site-to-Site VPN technology uses multiple alternative Internet connection at both ends of the connection, to provide aggregation and failover functions, so loss of Internet connectivity does not result in the interruption of the permanent connection.

Similarities and Relationships. There is often overlap between Dial-Up VPN technology and Site-to-Site technology, in that the VPN router or server may handle both Site-to-Site connectivity and accept Dial-Up VPN connections. In fact, Dial-Up VPN technology is at the foundation of the Site-to-Site VPN, in that the mechanics of establishing a site-to-site VPN involves making a dial-up type VPN connection between sites. The Site-to-Site VPN technology then builds on this by making each end of the VPN connection a router, thereby hiding the VPN from other devices on the network that may communicate across the connection. Site-to-Site VPN is similar to Persistent Dial-Up VPN technology, in that a VPN link is designed to be established and maintained perpetually, with advanced techniques to utilize redundant pathways and multiple Internet Service Providers on both ends. The key difference between Site-to-Site VPN and Persistent Dial-Up VPN is that with Persistent Dial-Up VPN, it is each individual workstation and laptop that initiates the connection into the network, rather than a separate VPN router device.

Peer-to-Peer VPN (Hamachi*)

Example. Hamachi* service by LogMeIn*.

Explanation. The basic idea of peer-to-peer VPN is to use a central coordinating server to help computers running proprietary VPN software locate each other, and communicate directly bypassing any central network. The central coordinating servers are sometimes to transmit data through them when firewall issues prevent the peers from being able to connect to each other directly. This

technology is more often utilized by gamers than by businesses, and being a P2P technology, does not allow for as much centralized control and administration as enterprise VPN systems typically provide. Also, since the coordinating servers are provided by a third party, this places more reliance on sending private data through a third-party service provider, which makes some risk analysts nervous or skeptical, even though sent information is at least in theory encrypted end-to-end.

Similarities and Relationships. Peer-to-Peer VPN is similar to Site-to-Site VPN in that it is designed to directly connect to like entities. Instead of connecting one site to another, it connects individual workstations to other workstations. The paid version of it is also similar to Persistent Dial-Up VPN in that it connects individual workstations to the network at boot time, making it available for remote access as soon as it is started up without requiring user login. The free version is similar to Dial-Up VPN in that a connection is designed to be established within a user session, and only for the duration of that session.

Persistent Dial-Up VPN (VPN Dialer)

Example. VPN Dialer by Onsitehelp Enterprise Software.

Explanation. Persistent Dial-Up VPN technology, like site-to-site VPN, builds on Dial-Up VPN technology, but performs the function at the individual computer level rather than at the site level. Rather than having each site use dedicated server or device for the purpose of maintaining a permanent VPN connection, each computer independently makes a permanent connection to the designated remote network. Since this technology is an extension of standard dial-up VPN technology, it uses the same PPTP, L2TP/IPSec, and SSTP connections as regular Dial-Up VPN.

Advanced implementations allow for configuring multiple Internet service providers and servers at the main network end, and multiple Internet service providers at the local end, and optimizing VPN connections based on measuring PING times, so loss of any server or Internet link results in a very quick re-acquisition of the connection, practically providing a robust permanent connection. Since each computer is responsible for maintaining a permanent connection, it allows a simplified architecture that uses only generic network equipment and Internet connectivity, but nonetheless robust and redundant end-to-end connectivity. There is a security benefit to this configuration over site-to-site VPN in that only computers configured to connect to the central network can communicate with that network. The corresponding disadvantage is that communicating with devices on remote networks will require using connected systems as intermediaries. In the future, devices can incorporate persistent dial-up VPN technology directly, so they can be accessed by the entire company without relying on an intermediary computer.

Similarities and Relationships. Persistent Dial-Up VPN is built on Dial-Up VPN technology. In fact, it uses the built-in Dial-Up VPN facility, to establish and maintain a VPN connection at all times (any time the computer is powered on and has Internet connectivity). It is similar to the paid version of Hamachi, in having individual computers establish a permanent link to a virtual network at boot time. But unlike Hamachi, Persistent Dial-Up VPN is not Peer to Peer technology. Computers connect to a designated central network, and when they communicate with each other, do so only through that central network. This technology is also similar to Site-to-Site VPN technology, in that it is built on Dial-Up VPN

technology, and uses it to maintain a permanent link. It is also similar in that multiple Internet providers can be configured at the server end and at the client end, to provide redundant and optimized links. Unlike Site-to-Site, there is no built-in support for acting as a router for other computers and devices on the same network. Under the Persistent Dial-Up technology model, each computer and device must make its own separate connection to the main network. If a particular device does not support Persistent Dial-Up VPN technology, then some method of tunneling information to the device must be implemented.

Comparison Table of Different VPN Technologies

	SSL VPN	Dial-Up VPN	Site-to-Site VPN	Peer-to-Peer VPN	Persistent Dial-Up VPN
Examples	Ovisgate	Windows RAS, Cisco VPN Client	Cisco, Windows RRAS	LogMeIn / Hamachi	VPN Dialer
Enterprise Focused Technology	Yes	Yes	Yes	No	Yes
Based on Open Standards	Yes	Yes	Yes	No	Yes
VPN Always Connected	No	No	Yes	Yes	Yes
Traditional VPN Concept	No	Yes	Yes	Yes	Yes
Access Non-Central LAN as if Local	No	No	Yes	Yes	No
End-to-End Redundancy Configuration Supported	No	No	Yes	No	Yes
Client-side Technology is:	Standard Web Browser	Software Bundled with Operating System	Standard TCP/IP; no VPN client needed.	Software as a Service (SaaS) with proprietary protocols	Licensed Software to Enhance Dial-Up VPN Functionality
Server-side Technology is:	Hardware Appliance or Software	Software Bundled with Server OS or Hardware Router	Hardware Router or Software Bundled with Server OS	Service Provider Proprietary	Same as Dial-Up VPN; tools to simplify VPN user management
Who Operates or “owns” the Infrastructure	Customer	Customer	Customer, ISP, or Phone Company	Service Provider	Customer