

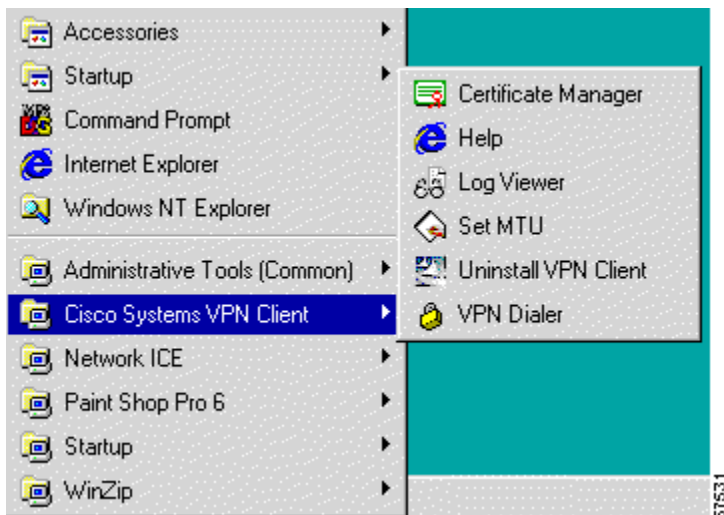
Understanding the Cisco VPN Client

The Cisco VPN Client for Windows (referred to in this user guide as *VPN Client*) is a software program that runs on a Microsoft® Windows®-based PC. The VPN Client on a remote PC, communicating with a Cisco Easy VPN server on an enterprise network or with a service provider, creates a secure connection over the Internet. Through this connection you can access a private network as if you were an on-site user. Thus you have a Virtual Private Network (VPN). The server verifies that incoming connections have up-to-date policies in place before establishing them. Cisco IOS, VPN 3000 Series Concentrators, and PIX central-site servers can all terminate VPN connections from VPN Clients.

As a remote user (low speed or high speed), you first connect to the Internet. Then you use the VPN Client to securely access private enterprise networks through a Cisco VPN server that supports the VPN Client.

The VPN Client comprises the following applications, which you select from the Programs menu:


Figure 1-1: VPN Client Applications as Installed by InstallShield



In logical order of use, the applications are as follows:

- Help—Displays an online manual with instructions on using the applications.

- VPN Dialer—Lets you configure connections to a VPN server and lets you then start your connections.
 - Certificate Manager—Lets you enroll for certificates to authenticate your connections to VPN servers.
 - Log Viewer—Lets you display events from the log.
 - Uninstall VPN Client—Lets you safely remove the VPN Client software from your system and retain your connection and certificate configurations.
-

 **Note** There are two ways to install the VPN Client: through the InstallShield wizard or through the Microsoft Installer. If you install the VPN Client through the Microsoft Installer, the Programs menu shown in Figure 1-1 does not contain the Uninstall application.

- SetMTU—Lets you manually change the size of the maximum transmission unit (see the *VPN Client Administrator Guide*, Chapter 6.)

How the VPN Client Works

The VPN Client works with a Cisco VPN server to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunneling protocols to make and manage the secure connection. Some of the steps include:

- Negotiating tunnel parameters—Addresses, algorithms, lifetime, and so on.
- Establishing tunnels according to the parameters.
- Authenticating users—Making sure users are who they say they are, by way of usernames, group names and passwords, and X.509 digital certificates.
- Establishing user access rights—Hours of access, connection time, allowed destinations, allowed protocols, and so on.

- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

For example, to use a remote PC to read e-mail at your organization, you connect to the Internet, then start the VPN Client and establish a secure connection through the Internet to your organization's private network. When you open your e-mail, the Cisco VPN server uses IPSec to encrypt the e-mail message. It then transmits the message through the tunnel to your VPN Client, which decrypts the message so you can read it on your remote PC. If you reply to the e-mail message, the VPN Client uses IPSec to process and return the message to the private network through the Cisco VPN server.

Connection Technologies

The VPN Client lets you use any of the following technologies to connect to the Internet:

- POTS (Plain Old Telephone Service)—Uses a dial-up modem to connect.
- ISDN (Integrated Services Digital Network)—May use a dial-up modem to connect.
- Cable—Uses a cable modem; always connected.
- DSL (Digital Subscriber Line)—Uses a DSL modem; always connected.

You can also use the VPN Client on a PC with a direct LAN connection.

VPN Client Features

The VPN Client includes the following features:

Program Features

- Complete browser-based context-sensitive HTML-based Help
- Support for VPN 3000 Series Concentrator platforms that run Release 3.0 and above. (VPN Client Release 3.0 and above will not work with Releases 2.x of the VPN 3000 Concentrator.)
- Command-line interface to the VPN Dialer

- Local LAN access—The ability to access resources on a local LAN while connected through a secure gateway to a central-site VPN server (if the central site grants permission)
- Automatic VPN Client configuration option—the ability to import a configuration file
- Log Viewer—An application that collects events for viewing and analysis
- Set MTU size—The VPN Client automatically sets a size that is optimal for your environment. However, you can set the MTU size manually as well. (For instructions on adjusting the MTU size, see the *VPN Client Administrator Guide*).
- Application Launcher—The ability to launch an application or a third-party dialer from the VPN Client.
- Automatic uninstall of the Nortel Networks VPN Client and the 5000 VPN Client software with the InstallShield installation package
- Automatic connection by way of Microsoft Dial-Up Networking or any other third-party remote access dialer
- Software update notifications from the VPN server upon connection
- Ability to launch a location site containing upgrade software from a VPN server notification
- The ability to automatically initiate secure wireless VPN connections seamlessly
- NAT Transparency (NAT-T), which lets the VPN Client and the VPN Concentrator automatically detect when to use IPSec over UDP to work properly in Port Address Translation environments.
- Update of centrally controlled backup server list—the VPN Client learns the backup VPN Concentrator list through connection establishment. This feature is configured on the VPN 3000 Concentrator and pushed to the VPN Client. The addresses show in the VPN Dialer application in the Enable Backup Servers box under Options->Properties->Connections.
- Support for Dynamic DNS (DDNS hostname population)—The VPN Client sends its hostname to the VPN Concentrator during connection

establishment. The VPN Concentrator can send the hostname in a DHCP request that can cause a DNS server to update its database to include the new hostname and Client address.

Windows NT, Windows 2000, and Windows XP Features

- Password expiration information when authenticating through a RADIUS server that references an NT user database. When you log in, the VPN Concentrator sends a message that your password has expired and asks you to enter a new one and then confirm it. On pre-Release 3.5 VPN Clients, the prompt asks you to supply a PIN and to verify it. On a 3.5 or above VPN Client, the prompt asks you to enter and verify a password.
- Start Before Logon—The ability to establish a VPN connection before logging on to a Windows NT platform, which includes Windows NT 4.0, Windows 2000, and Windows XP systems.
- Ability to disable automatic disconnect when logging off of a Windows NT platform. This allows for roaming profile synchronization.

IPSec Features

- IPSec tunneling protocol
- Transparent tunneling—IPSec over UDP for NAT and PAT, and IPSec over TCP for NAT, PAT, and firewalls
- IKE key management protocol
- IKE Keepalives—Monitoring the continued presence of a peer and reporting the VPN Client's continued presence to the peer. This lets the VPN Client notify you when the peer is no longer present. Another type of keepalives keeps NAT ports alive.
- Split tunneling—The ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel. The VPN Server supplies a list of networks to the VPN Client for tunneled traffic. You enable split tunneling on the VPN Client and configure the network list on the VPN Server, such as the VPN Concentrator.
- Support for Split DNS—The ability to direct DNS packets in clear text over the Internet to domains served through an external DNS (serving your ISP) or through an IPSec tunnel to domains served by the corporate DNS.

The VPN Server supplies a list of domains to the VPN Client for tunneling packets to destinations in the private network. For example, a query for a packet destined for *corporate.com* would go through the tunnel to the DNS that serves the private network, while a query for a packet destined for *myfavoritesearch.com* would be handled by the ISP's DNS. This feature is configured on the VPN Server (VPN Concentrator) and enabled on the VPN Client by default. To use Split DNS, you must also have split tunneling configured.


- LZS data compression, which can benefit modem users

Authentication Features

- User authentication by way of VPN central-site device:
 - - Internal through the VPN device's database
 - RADIUS (Remote Authentication Dial-In User Service)
 - NT Domain (Windows NT)
 - RSA (formerly SDI) SecurID or SoftID
 - Certificate Manager—An application that lets you manage your identity certificates
 - Ability to use Entrust Entelligence certificates
 - Ability to authenticate using smart cards with certificates
 - Peer Certificate Domain Name Verification—prevents a client from connecting to a invalid gateway by using a stolen but valid certificate and a hijacked IP address. If the attempt to verify the domain name of the peer certificate fails, the client connection also fails.

Firewall Features

- Support for Cisco Secure PIX Firewall platforms that run Release 6.0 and higher
-

 **Note** Instructions on configuring the VPN Client to interoperate with Cisco Secure PIX Firewall, Release 6.0 and above, are available in *IPSec User Guide for Cisco Secure PIX Firewall*.

- Support for personal firewalls:
 - - Cisco Integrated Firewall (CIC)
 - ZoneAlarmPro 2.6.3.57
 - ZoneAlarm 2.6.3.57
 - Zone Integrity
 - BlackIce Agent and BlackIce Defender 2.5
- Centralized Protection Policy—Support for firewall policies pushed to the VPN Client from a VPN Concentrator

VPN Client IPSec Attributes

The VPN Client supports these IPSec attributes:

- Main mode for negotiating phase one of establishing ISAKMP Security Associations (SAs)
- Aggressive mode for negotiating phase one of establishing ISAKMP SAs
- Authentication algorithms:
 - - HMAC (Hashed Message Authentication Coding) with MD5 (Message Digest 5) hash function
 - HMAC with SHA-1 (Secure Hash Algorithm) hash function
- Authentication Modes:
 - - Preshared Keys

- X.509 Digital Certificates
 - Diffie-Hellman Groups 1(for digital certificates), 2, and 5
 - Encryption algorithms:
 - - 56-bit DES (Data Encryption Standard)
 - 168-bit Triple-DES
 - AES 128-bit and 256-bit
-

 **Note** You must be running Release 3.6 of the VPN Client to use the AES encryption algorithm

- Extended Authentication (XAUTH)
- Mode Configuration (also known as ISAKMP Configuration Method)
- Tunnel Encapsulation Mode
- IP compression (IPCOMP) using LZS