

Q. Where can I download the VPN Client software?

A. You **must** log in and possess a valid service contract in order to access the VPN Client software. VPN Client software can be downloaded from the [Software Center](#) (registered customers only) .

If you do not have a valid service contract associated with your Cisco.com profile you cannot log in and download the VPN Client software.

Follow these steps to obtain a valid service contract:

Contact your Cisco Account team if you have a Direct Purchase Agreement.

[Contact](#) a Cisco Partner or Reseller in order to purchase a service agreement.

Use the [Profile Manager](#) (registered customers only) in order to update your Cisco.com profile and request association to a service agreement.

Q. The VPN Client download area appears to be empty. Why?

A. When you reach the [VPN Client area of the Software Center](#) (registered customers only) be sure that you select the downloads area for your desired operating system in the middle of the page.

Q. How can I disable the Stateful Firewall Feature during the installation of the VPN Client?

A. Refer to the [Documentation Changes](#) section of the [VPN Client Rel 4.7 Release Notes](#) in order to learn about the two topics "Using MSI to Install the Windows VPN Client without Stateful Firewall" and "Using InstallShield to Install the Windows VPN Client without Stateful Firewall".

Q. How do I unistall or upgrade the Cisco VPN Client?

A. Refer to the [How to Uninstall Manually and Upgrade the Cisco VPN Client 3.5 and Later for Windows 2000 and Windows XP](#) in order to know the procedure to manually uninstall (InstallShield) and then upgrade the Cisco VPN Client Version 3.5 and later for Windows 2000 and Windows XP.

Q. I want to customize the VPN-Clients for Vista. Now I recognize that, with the new VPN-Client Version for Vista, there is no file such as oem.mst. How can we customize the new VPN-Client-Versions (5.x), or where I can find this file?

A. The MST file is no longer provided with the VPN Client, but you can download it from the [Software Center](#) (registered customers only) :

Filename: Readme and MST for installation on the international version of Windows.

Q. Does the Cisco VPN client have the capability to automatically start/terminate based on when an application (ie. Outlook) launches/closes?

A. The VPN client doesn't have such a capability. You can only launch scripts before and after VPN start/termination.

Documentation

Q. Where is the VPN Client documentation found?

A. On [CCO](#).

Operating System

Q. Is the Cisco VPN Client supported on 64-bit platforms?

A. Not at this time. If you want 64-bit support please use the AnyConnect SSL VPN client at this time. If you try to install the Cisco IPsec VPN client on a 64-bit machine it will error out with a message and not allowed to proceed with the installation

Update:Yes, VPN Client v5.0.7 supports Windows 7 and Vista 64-bit platforms. See [Release Notes](#) for details.

Q. Is the Cisco VPN Client supported on VMware or other virtualized software ?

A. The VPN Client doesn't support any virtualized software at this time.

Q. Does Cisco provide a VPN Client for Windows Vista?

A. Cisco VPN Client Version 5 is available for 32-bit Windows Vista. Support for 64-bit Windows Vista is not available at this time. This client and release notes can be obtained from the [Software Center](#) (registered customers only) .

Update: Yes, VPN Client v5.0.7 supports Windows 7 and Vista 64-bit platforms. See [Release Notes](#) for details.

Note: Cisco VPN Client is only supported on Windows Vista clean install. It means that an upgrade of Windows of any OS to Windows Vista is not supported with the VPN Client Software of this Vista. You must freshly install the Windows Vista and try to install the Vista VPN Client software.

Note: If you do not have a valid service contract associated with your Cisco.com profile you cannot log in and download the VPN Client software. See [Download VPN Client Software](#) for more information.

Tip: The Cisco AnyConnect VPN Client is now available for the Windows Operating Systems, which includes Vista 32 and 64-bit. The AnyConnect client supports SSL and DTLS. It does not support IPSec at this time. Additionally, AnyConnect is available only for use with a Cisco Adaptive Security Appliance that runs version 8.0(2) or later. The client can also be used in weblaunch mode with IOS appliances running version 12.4(15)T. VPN 3000 is not supported.

The Cisco AnyConnect VPN Client and ASA 8.0 can be obtained from the [Software Center](#) (registered customers only) . Refer to the [Cisco AnyConnect VPN Client Release Notes](#) for more information on the AnyConnect Client. Refer to the [Cisco ASA 5500 Series Adaptive Security Appliances Release Notes](#) for more information on ASA 8.0.

Note: If you do not have a valid service contract associated with your Cisco.com profile you cannot log in and download the AnyConnect VPN Client or ASA software. See [Download VPN Client Software](#) for more information.

Q. How do I set up a PPTP connection from a Microsoft Windows PC?

A. Setup depends on the version of Microsoft Windows that you run. You should contact Microsoft for specific information. These are setup instructions for some of the common versions of Windows.

Windows 95

1. Install Msdun13.exe.
2. Choose **Programs > Accessories > Dial Up Networking**.
3. Create a new connection called "PPTP."
4. Select the **VPN Adapter** as the device for the connection.
5. Enter the IP address of the public interface of the switch and click **Finish**.
6. Go back to the connection that you have just created, click the right mouse button, and choose **Properties**.
7. Under Allowed Network Protocols, at minimum, and uncheck **netbeui**.
8. Configure the **Advanced Options** setting:
 1. Leave default settings to allow the switch and client to auto-negotiate the authentication method.
 2. Enable **Require Encrypted Password** to force Challenge Handshake Authentication Protocol (CHAP) authentication.
 3. Enable **Require Encrypted Password** and **Require Data Encryption** to force MS-CHAP authentication.

Windows 98

1. Follow these steps to install the PPTP feature.

1. Choose **Start > Settings > Control Panel > Add New Hardware**. Click **Next**.
2. Click **Select from List** and choose **Network Adapter**. Click **Next**.
3. Choose **Microsoft** in the left panel and **Microsoft VPN Adapter** on the right panel.
2. Follow these steps to configure the PPTP feature.
 1. Choose **Start > Programs > Accessories > Communications > Dial Up Networking**.
 2. Click **Make new connection** and for **Select a device**, connect using **Microsoft VPN Adapter**. The VPN Server IP address= 3000 tunnel endpoint.
3. Complete these steps to change the PC to also allow Password Authentication Protocol (PAP).

Note: The Windows 98 default authentication is to use password encryption (CHAP or MS-CHAP).

 1. Choose **Properties > Server types**.
 2. Uncheck **Require encrypted password**. You can configure data encryption (Microsoft Point-to-Point Encryption [MPPE] or no MPPE) in this area.

Windows 2000

1. Choose **Start > Programs > Accessories > Communications > Network and Dialup connections**.
2. Click **Make new connection** and then click **Next**.
3. Select **Connect to a private network through the Internet and Dial a connection prior** (do not select this if you have a LAN). Click **Next**.
4. Enter the hostname or IP address of tunnel endpoint (3000).
5. If you need to change the password type, select **Properties > Security for the connection > Advanced**. The default is MS-CHAP and MS-CHAP v2 (not CHAP or PAP). You can configure data encryption (MPPE or no MPPE) in this area.

Windows NT

Refer to [Installing, Configuring, and Using PPTP with Microsoft Clients and Servers](#).

Q. What operating system versions support the Cisco VPN Client?

A. Support for additional operating systems is constantly added for the VPN Client. Refer to the system requirements in the release notes for the latest client to determine this, or refer to [Cisco Hardware and VPN Clients Supporting IPsec/PPTP/L2TP](#).

Q. Do I need to be an Administrator on Windows NT/2000 machines in order to load the VPN Client?

A. Yes, you must have Administrator privileges to install the VPN Client on Windows NT and Windows 2000 because these operating systems require Administrator privileges to bind to the existing network drivers or to install new network drivers. The VPN Client software is networking software. You must have Administrator privileges to install it.

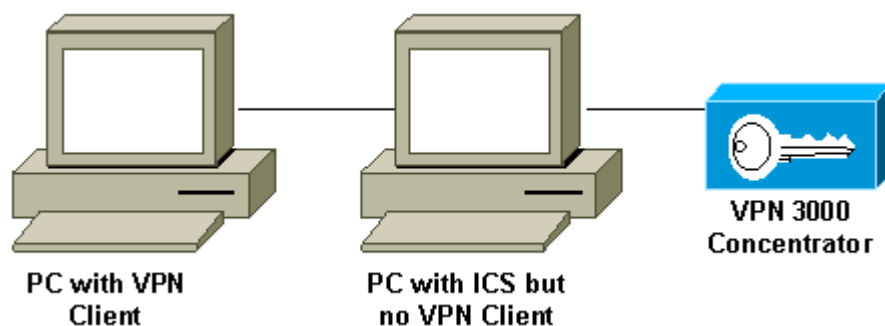
Q. Is a reboot required after installing the VPN Client?

A. Yes.

Q. Can the Cisco VPN Client work with Microsoft Internet Connection Sharing (ICS) installed on the same machine?

A. No, the Cisco VPN 3000 Client is not compatible with Microsoft ICS on the same machine. You must uninstall ICS before you can install the VPN Client. Refer to [Disabling ICS when Preparing to Install or Upgrade to Cisco VPN Client 3.5.x on Microsoft Windows XP](#) for more information.

Although having the VPN Client and ICS on the same PC does not work, this arrangement does work.



Q. My VPN Client seems to only connect to certain addresses. I run Windows XP. What should I do?

A. Verify that the built-in firewall in Windows XP is disabled.

Q. Is the Cisco VPN Client compatible with the Windows XP stateful firewall?

A. This issue has been resolved. View Cisco bug ID [CSCdx15865](#) (registered customers only) in Bug Toolkit for more details.

Q. When I install the VPN Client on Windows XP and on Windows 2000, is the multi-user interface disabled?

A. The installation disables the welcome screen and the fast user switching. View Cisco bug ID [CSCdu24073](#) (registered customers only) in Bug Toolkit for more details.

Q. How can I make the VPN Client for Linux move to the background after execution? If I initiate a connection such as `vpnclient connect foo`, I get in, but the shell is returned.

A. After signing on, type these.

`^Z`

`bg`

Q. When I install the Cisco VPN Client on Windows XP Home Edition, the task bar is not visible. How do I undo this?

A. Choose Control Panel > Network Connections > Remove Network Bridge to adjust this setting.

Q. While I attempt to install Linux VPN Client on RedHat 8.0, I get an error that says the module cannot be loaded because the module was compiled with GCC 2 and the kernel was compiled with GCC 3.2. What should I do?

A. This is because the new release of RedHat has a newer version of the GCC compiler (3.2+), which causes the current Cisco VPN Client to fail. This issue has been fixed and is available in Cisco VPN 3.6.2a. View Cisco bug ID [CSCdy49082](#) (registered customers only) in Bug Toolkit for more details or download the software from the [VPN Software Center](#) (registered customers only).

Q. Why does the software disable Fast User Switching when you install VPN Client 3.1 on Windows XP?

A. Microsoft automatically disables Fast User Switching in Windows XP when a GINA.dll is specified in the registry. The Cisco VPN Client installs the CSgina.dll to implement the "Start Before Login" feature. If you need Fast User Switching, then disable the "Start Before Login" feature. Registered users can get more information in Cisco bug ID [CSCdu24073](#) (registered customers only) in Bug Toolkit.

Error Messages

Q. When I install VPN Client 4.x, I receive this error message: "Warning 201: The necessary VPN sub-system is not available. You can not connect to the remote VPN server"

A. This issue can be caused by firewall packages installed on your VPN client computer. In order to avoid this error message, ensure that no firewall or antivirus programs are installed or running on your PC at the time of installation.

Q. I upgraded to Mac OS X 10.3 (known as "Panther"), but now my VPN Client 4.x displays an error that states: "Secure VPN Connection terminated locally by the Client Reason: Unable to contact the security gateway"

A. You must add UseLegacyIKEPort=0 to the profile (.pcf file) found in the /etc/CiscoSystemsVPNClient/Profiles/ directory for the VPN Client 4.x to work with Mac OS X 10.3 ("Panther").

Q. What does it mean when I get "Error msg: failed to find the uninstall file..." while I try to uninstall the VPN Client? Also, what needs to be done to successfully complete the uninstallation?

A. Check the networking Control Panel to ensure that the Deterministic NDIS Extender (DNE) was not installed. Also choose **Microsoft > Current Version > Uninstall** in order to check for the uninstall file. Remove the

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Uninstall\{5624C000-B109-11D4-9DB4-00E0290FCAC5} file and retry the uninstallation.

Q. I cannot install the VPN Client on Windows 2000 Professional. I get the error: "An installation support file could not be installed" Catastrophic Failure. What should I do?

A. Remove the **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall** key. Then reboot your computer, and reinstall the VPN Client.

Note: In order to find the correct key for the Cisco VPN Client software under the path **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall\<key to be determined>**, go to the path **HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems** and click **VPN Client**. In the right-hand window, you see the Uninstall Path (under the Name column). The corresponding Data column displays the VPN Client Key value. You need to take this key as reference and go to the path **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Currentversion\Uninstall**. Then select the determined key and delete it.

Refer to [Initialization Error Troubleshooting](#) and refer to Cisco bug ID [CSCdv15391](#) (registered customers only) in Bug Toolkit for more information.

Q. While I attempt to install Linux VPN Client on RedHat 8.0, I get an error that says the module cannot be loaded because the module was compiled with GCC 2 and the kernel was compiled with GCC 3.2. What should I do?

A. This is because the new release of RedHat has a newer version of the GCC compiler (3.2+), which causes the current Cisco VPN Client to fail. This issue has been fixed and is available in Cisco VPN 3.6.2a. View Cisco bug ID [CSCdy49082](#) (registered customers only) in Bug Toolkit for more details or download the software from the [VPN Software Center](#) (registered customers only) .

Q. I get a "peer no longer responding" error message when my Linux Client 3.5 tries to establish an IPsec connection to a PIX or to a VPN 3000 Concentrator. What should I do?

A. The symptom of this problem is that the Linux Client seems to try to connect, but it never gets a response from the gateway device.

The Linux OS has a built-in firewall (ipchains) that blocks UDP port 500, UDP port 1000, and Encapsulating Security Payload (ESP) packets. Since the firewall is on by default, you either have to disable the firewall or open up the ports for IPsec communication for both inbound and outbound connections to fix the problem.

Q. I receive a kernel extension error when I try to run Cisco VPN 5000 5.2.2 Client on Mac OS X 10.3. What should I do?

A. As stated in the product [release notes](#), the Cisco VPN 5000 Client is supported up to version 10.1.x and thus is not supported on version 10.3. It is possible to make the VPN Client work when you reset the permissions on two of the installed files after you run the install script. This is an example.

Note: This configuration is *not* supported by Cisco.

```
sudo chown -R root:wheel /System/Library/Extensions/VPN5000.kext
sudo chmod -R go-w /System/Library/Extensions/VPN5000.kext
```

Q. I am unable to install the new version of VPN Client. I get an error message "Error DNEinst execution error while installing DNE, return code -2146500093" or "InstallDNE Error: DNEinst execution error while installing DNE, returncode -2147024891" while I install. This happened while I installed the Deterministic Network Enhancer.

A. Install the latest DNE upgrade from [Deterministic Networks](#) .

Q. I get these logs on the VPN Client while I make a connection:

```
208    15:09:08.619    01/17/08    Sev=Debug/7          CVPND/0x63400015
Value for ini parameter VAEnableAlt is 1.

209    15:09:08.619    01/17/08    Sev=Warning/2       CVPND/0xE3400003
Function RegOpenKey failed with an error code of
0x00000002(WindowsVirtualAdapter:558)

210    15:09:08.619    01/17/08    Sev=Warning/3       CVPND/0xE340000C
The Client was unable to enable the Virtual Adapter because it
could not open the device.
```

A. It is a fairly generic error message, which usually requires manual uninstallation of the client. Follow the instructions in this link. [How to Uninstall Manually and Upgrade the Cisco VPN Client 3.5 and Later for Windows 2000 and Windows XP.](#)

Once you have done the uninstall, make sure you reboot. Then reinstall the client. Make sure you are logged on as a user that has admin rights on the local machine.

Q. When I attempt to connect the VPN, I get this error message on the MAC OS for Cisco VPN client: "Error 51- Unable to communication with the VPN subsystem."

A. The issue can be resolved if you restart the service after you close the VPN client in this way:

To stop:

```
sudo kextunload -b com.cisco.nke.ipsec
```

To start:

```
sudo kextload /System/Library/Extensions/CiscoVPN/CiscoVPN
```

Third Party Compatability

Q. Is the Nortel or other third-party VPN Client compatible with the Cisco VPN 3000/ASA Concentrators?

A. No. The Nortel and other third-party VPN Clients cannot connect to the Cisco VPN 3000/ASA Concentrator.

Q. Can I have VPN Clients from other vendors, such as the Nortel Contivity VPN Client, installed simultaneously with the Cisco VPN Client?

A. Yes. As of Release 4.0, the VPN Client is compatible with VPN clients from Microsoft, Nortel, Checkpoint, Intel, and others. This feature offers the ability to use other VPN products while the Cisco VPN Client is installed.

Q. Are Cisco VPN Clients supported with third party VPN Concentrators?

A. Cisco VPN Clients are not supported with third party VPN Concentrators.

Authentication

Q. How do VPN Clients 1.1 and 3.x internally store digital certificates (X.509v3)?

A. The VPN Client 1.1 has its own certificate store. The VPN Client 3.x can either store certificates in the Microsoft store using Common-Application Programming Interface (CAPI), or it can store them in Cisco's own store (RSA Data Security).

Q. Does the VPN IPsec Client have the capability to display a message/warning to the end user when the client's digital certificate is about to expire in X future days?

A. Yes, the VPN IPsec client will warn the user when the certificate is about to expire, starting 30 days prior to expiration. There's no configuration setting to disable the certificate expiration popup. Renewing the certificate will cause the popup to not display.

Q. Can I have the same groupname and username on the VPN Concentrator?

A. No, groupname and username cannot be the same. This is a known issue, found in software versions 2.5.2 and 3.0, and integrated into 3.1.2. View Cisco bug ID [CSCdw29034](#) (registered customers only) in Bug Toolkit for more information.

Q. Are full-challenge cards such as the Defender supported on the Cisco VPN Client to PIX/VPN 3000/ASA?

A. No, cards of this type are not supported.

Q. Can the VPN Client automatically login/authenticate to the security appliance using the Windows credentials, thus not requiring user interaction?

A. No this is not supported. We recommend you use digital certificates for authenticating the VPN session without the need for enduser interaction.

VPN Client Software Version

Q. What happened to the "Set MTU Utility" option that was in VPN Client versions 2.5.2 and earlier?

A. The VPN Client now adjusts the Maximum Transmission Unit (MTU) size. The Set MTU Utility option is no longer a required installation step and has been removed from the Start menu. Use Internet Explorer in order to access the Set MTU Utility option. You can also choose **Start > Run**, choose **Browse**, and navigate to the Cisco Systems VPN Client directory.

Q. What personal firewalls are supported with the Cisco VPN Client?

A. Refer to the System Requirements in the release notes for your VPN Client to determine interoperability issues or support of personal firewalls. Starting in version 3.1, a new feature is added to the VPN 3000 Concentrator that detects what personal firewall software remote users have installed and prevents the users from connecting in the absence of the appropriate software. Select **Configuration > User Management > Groups > Client FW** and select the tab for the group to configure this feature.

Q. Are there connectivity issues when using the VPN Client 3.x with AOL 7.0?

A. The VPN Client does not work with AOL 7.0 without the use of split tunneling. View Cisco bug ID [CSCdx04842](#) (registered customers only) in Bug Toolkit for more details.

VPN Client Software Configuration

Q. Why does the VPN Client disconnect after 30 minutes? Can I extend this time period?

A. If there is no communication activity on a user connection during this 30-minute period, the system terminates the connection. The default idle timeout setting is 30 minutes, with a minimum allowed value of 1 minute and a maximum allowed value of 2,147,483,647 minutes (more than 4,000 years).

Choose **Configuration > User Management > Groups** and choose the appropriate group name to modify the idle timeout setting. Select **Modify Group**, go to the HW Client tab, and type the desired value in the User Idle Timeout field. Type to disable timeout and allow an unlimited idle period.

Q. Can the Cisco VPN Client be deployed with all the parameters preconfigured?

A. Yes. Administrators can create a Cisco VPN Client installation floppy disk set that has all client configuration parameters preset so that the installation is completely hands-free for end users. Information related to the creation of a predefined configuration is noted in the [Cisco VPN Client documentation](#).

Q. It seems like the VPN Client has a conflict with my NIC card. How should I troubleshoot this?

A. Make sure that you run the latest drivers on the NIC card. This is always recommended. If possible, test to see if the problem is specific to the operating system, PC hardware, and other NIC cards.

Q. How do I automate the VPN Client connection from Dial-Up Networking?

A. Choose **Options > Properties > Connections**, and have the VPN Client pull down a Dial-Up Networking phone book entry in order to fully automate the dial-up into the VPN connection.

Q. How do I configure the Cisco VPN 3000 Concentrator to notify remote users for VPN Client update?

A. Refer to [Notifying Remote Users of a Client Update](#). Ensure that you type the release information as "(Rel)", as noted in step 6 of the process.

Q. What can cause a delay before the VPN Client appears, specifically when the "Start Before Logon" option is enabled?

A. The VPN Client is in "fall back" mode. This contributes to the delay. Uninstall the VPN Client and remove the offending applications to allow startup without being in "fall back" mode. Then reinstall the VPN Client. View Cisco bug IDs [CSCdt88922](#) (registered customers only) and [CSCdt55739](#) (registered customers only) in Bug Toolkit for more information.

Q. I need to understand the difference between ipsecdialer.exe and vpngui.exe. Why is vpngui.exe installed in STARTUP in my Windows XP but I still have to manually start ipsecdialer in order to reach my companies resources? And (apart from the size) these programs seem to trigger the same thing which is a VPN logon to my company network.

A. The ipsecdialer.exe was the original launching mechanism for VPN Client 3.x. When the GUI was changed in the 4.x versions, a new executable called vpngui.exe was created. The ipsecdialer.exe file was carried forward in name only for backward compatibility and just launches the vpngui.exe. This is the reason you could see the difference in the file size. So when you downgrade from the 4.x to the 3.x VPN Client, you need the ipsecdialer.exe file to launch this.

Q. Can I safely remove the startup VPN icon? Why is it needed?

A. The VPN Client in the startup folder supports the "Start Before Logon" feature. If you do not use the feature, then you do not need it in the startup folder.

Q. Why is "user_logon" added and not at the ipsecdialer.exe shortcut? What is the purpose of "user_logon"?

A. The "Start Before Logon" feature requires the "user_logon" but a normal launch of the VPN Client by the user does not need this.

NAT/PAT Problems

Q. I am experiencing problems with only one VPN Client (for releases 3.3 and earlier) being able to connect through a Port Address Translation (PAT) device. What can I do to alleviate this problem?

A. There was a bug in several Network Address Translation (NAT)/PAT implementations that causes ports less than 1024 not to be translated. On the VPN Client 3.1, even with NAT transparency enabled, the Internet Security Association and Key Management Protocol (ISAKMP) session uses UDP 512. The first VPN Client goes through the PAT device and keeps source port 512 on the outside. When the second VPN Client connects, port 512 is already in use. The attempt fails.

There are three possible workarounds.

Fix the PAT device.

Upgrade the VPN Clients to 3.4 and use TCP encapsulation.

Install a VPN 3002 that replaces all VPN Clients.

Q. Can two laptops be connected with the VPN Client from the same location?

A. Two clients can connect to the same head end from the same location as long as the clients are not both behind a device performing PAT such as a SOHO router/firewall. Many PAT devices can map ONE VPN connection to a client behind it, but not two. In order to allow two VPN clients to connect from the same location behind a PAT device, enable some sort of encapsulation such as NAT-T, IPsec over UDP, or IPsec over TCP at the head end. Generally, NAT-T or another encapsulation should be enabled if ANY NAT device is between the client and the head end.

Miscellaneous

Q. When I connect to the network in the office using my laptop and then take the laptop home, I have trouble connecting to the VPN 3000 Concentrator from home. What is the problem?

A. The laptop might be retaining the routing information from the LAN connection. Refer to [VPN Clients with Microsoft Routing Problems](#) for information about how to resolve this issue.

Q. How can I tell if a VPN Client is connected to the VPN Concentrator?

A. Check the registry key named HKLM\Software\Cisco Systems\VPN Client\TunnelEstablished. If a tunnel is active, the value is 1. If no tunnel is present, the value is 0.

Q. I have problems with the NetMeeting connection from a PC behind a VPN Concentrator to a VPN Client, but the connection works when I run from the PC to a VPN Client behind a VPN Concentrator. How can I resolve this?

A. Follow the appropriate step(s) listed here in order to control the connection settings.

On the main drive of the PC, choose **Program Files > Cisco Systems > VPN Client > Profiles**. Right-click on the profile that you use and choose **Open With** from the sub-menu to open the profile in a program like Notepad. (When you choose the program to use, be sure to uncheck the box that says **Always use this program to open these files**.) Locate the profile parameter for ForcekeepAlives and change the value from 0 to 1, then save the profile.

or

For the VPN Client, choose **Options > Properties > General** and enter a value for the "Peer response timeout", as shown in this [sample window](#). You can specify a timeout sensitivity of 30 seconds to 480 seconds.

or

For the VPN Concentrator, choose **Configuration > User Management > Groups > modify group**. On the IPsec tab, select the option for IKE Keepalives, as shown in this [sample window](#).

The Dead Peer Detection (DPD) interval varies based on the sensitivity setting. Once a response is not received, it moves into a more aggressive mode, and sends packets every five seconds until the peer response threshold is met. At that time, the connection is torn down. You can disable the keepalives, but if your connection does actually drop, you need to wait for the timeout. Cisco recommends that you set the sensitivity value very low initially.

Q. Can you establish multiple IPsec remote access sessions from the same PC to two different VPN headend concentrators?

A. No, this is not a supported or operational configuration. Only one IPsec remote access session can be sourced from a PC endpoint.

Related Information

[Cisco VPN 3000 Client Support Page](#)

[Cisco VPN Client Support Page](#)

[Most Common L2L and Remote Access IPsec VPN Troubleshooting Solutions](#)

[Technical Support & Documentation - Cisco Systems](#)

[Cisco VPN Client FAQ](#)