



# Release Notes for VPN Client, Release 4.9.00.0050 for Mac OS X

---

**Revised: May 27, 2011**

These release notes support Cisco VPN Client software, Release 4.9.00.0050 for Mac OS X. Please refer to [About Version Numbers, page 3](#) for information about the version numbering scheme.

The 4.9.00.0050 VPN Client for Mac OS X is the first version to support the Intel processor for Mac OS X.

This VPN Client release for Mac OS X supports *only* OS X 10.4 and 10.5 on both Power PC (PPC) and Intel processors. This version does *not* support earlier or later versions.

These release notes describe new features, limitations and restrictions, caveats, and related documentation. Please read the release notes carefully prior to installation. The section, “Usage Notes,” describes interoperability considerations and other issues you should be aware of when installing and using the VPN Client. Where applicable, caveat identifiers appear in parentheses following new feature descriptions and usage notes.

## Contents

[Introduction, page 2](#)

[System Requirements, page 2](#)

[Installation Notes, page 3](#)

[New Feature in Release 4.9, page 4](#)

[Usage Notes, page 4](#)

[Open Caveats, page 9](#)

[Resolved Caveats in VPN Client for Mac OS X, Release 4.9.00.0050, page 34](#)

[Documentation Updates, page 34](#)

[Related Documentation, page 36](#)



---

**Americas Headquarters:**  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

## Introduction

The VPN Client is an application that runs on a Macintosh (Mac) personal computer that meets the system requirements stated in the next section. In this document, the term “PC” applies generically to all these computers, unless specified otherwise.

The VPN Client on a remote PC, communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. This secure connection is a Virtual Private Network (VPN).

## System Requirements

Refer to Chapter 2, “Installing the VPN Client,” in the *Cisco VPN Client User Guide for Mac OS X* for a complete list of system requirements and installation instructions.

- To install the VPN Client on *any* system, you need
  - CD-ROM drive (if you are installing from CD-ROM)
  - Administrator privileges
- The following table shows the supported platforms.

Computer	Operating System	Requirements
Computer with a Pentium®-class processor or greater, including TabletPC 2004/2005	The 4.9.00.0050 VPN Client for Mac OS X is the first version to support the Intel processor for Mac OS X.  This VPN Client release for Mac OS X supports <i>only</i> OS X 10.4 and 10.5 on both PPC and Intel processors. This version does <i>not</i> support Mac OS X earlier and later releases.	<ul style="list-style-type: none"> <li>• 50 MB hard disk space.</li> <li>• PPC or Intel processor.</li> </ul>
Macintosh computer	Mac OS X, Version 10.4 or 10.5	

The VPN Client supports the following Cisco VPN devices:

- Cisco VPN 3000 Series Concentrator, Version 3.0 and later. Using IPsec over TCP requires VPN 3000 Series Concentrator version 3.6.7.a and later.
- Cisco PIX Firewall, Version 6.2.2(122) or Version 6.3(1).
- Cisco IOS Routers, Version 12.2(8)T and later

VPN Client does not support the establishment of a VPN connection over a tethered link.

If you are using Internet Explorer, use version 5.0, Service Pack 2 or higher.

# Installation Notes

The following sections list information relevant to installing and using the VPN Client release 4.9.00.50 for the Mac OS X platforms:

- [File in VPN Client for Mac OS X, Release 4.9.00.0050, page 3](#)
- [Using the VPN Client, page 3](#)
- [About Version Numbers, page 3](#)

## File in VPN Client for Mac OS X, Release 4.9.00.0050

The VPN Client for Mac OS X, Release 4.9.00.0050 consists of the following file:

vpnclient-darwin-4.9.00.0050-k9.dmg

## Using the VPN Client

- To use the VPN Client, you need
  - Direct network connection (cable or DSL modem and network adapter/interface card), or
  - Internal or external modem
- To connect using a digital certificate for authentication, you need a digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:
  - Baltimore Technologies ([www.baltimoretechnologies.com](http://www.baltimoretechnologies.com))
  - Entrust Technologies ([www.entrust.com](http://www.entrust.com))
  - Netscape ([www.netscape.com](http://www.netscape.com))
  - Verisign, Inc. ([www.verisign.com](http://www.verisign.com))

## About Version Numbers

Beginning with the VPN Client 4.6 release, an all-numeric version numbering system has been adopted for VPN Client software to facilitate the automatic update function. Release numbers are represented in the format:

<major release>.<minor release>.<sustaining release>.<build>

The major and minor release numbers represent the feature level of the product. Major and minor releases implement new product capabilities. The sustaining and build release numbers represent significant or minor patch levels, respectively. For example, 4.9.00.0050 represents feature release 4.9, build 50.

All sustaining and build releases are cumulative, and not all build numbers will be released externally. These release notes specify the released build number.

## New Feature in Release 4.9

The VPN Client for Mac OS X now supports the Intel processor for Mac OS X. This VPN Client release for Mac OS X supports *only* OS X 10.4 and 10.5 on both PPC and Intel processors. It does *not* support earlier and later releases.

## API for Cisco VPN Client

The Cisco VPN Client offers an application programming interface (API). The software, sample program, and documentation are available at <http://www.cisco.com/cgi-bin/tablebuild.pl/windows>, along with the rest of the VPN Client downloads. The file name is APIExample\_Rev4.zip.

If you do not have a CCO account, please visit <http://tools.cisco.com/RPF/register/register.do> and register for a guest account. Once you have done this forward the account ID to the [vpn-client-api-support@cisco.com](mailto:vpn-client-api-support@cisco.com) so that we can publish the file to you.

**Note**

---

The Solaris VPN Client does not provide API support.

---

All API commands require that the 4.6.x and later of the VPN Client be fully installed.

If you are planning on using C, we recommend you call the `vpnapi.dll` directly; however, if you plan on using C++, then use the example provided in the zip file. The example is compatible with Visual Studio 2005. The documentation in the zip file will work for both C & C++.

## Usage Notes

This section lists issues to consider before installing Release 4.9 of the VPN Client software.

In addition, you should be aware of the open caveats regarding this release. Refer to [“Open Caveats” on page 9](#) of these Release Notes for the list of known problems.

## 64-bit Kernel Mode Not Supported

Cisco VPN Client does not support Mac OS X 64-bit kernel mode. Either use the embedded Apple VPN client or reconfigure the Mac to boot in 32-bit mode.

## Cannot Connect to ASAs Using the Same FQDN with TCP

VPN Client cannot complete a VPN connection if it is using IPsec over TCP and two or more ASAs are using the same FQDN.

As a workaround, use IPsec over UDP or plain IPsec, or upgrade to Cisco AnyConnect Secure Mobility client, release 2.5(3), 3.0(2), or later.

## Selecting “Send CA Certificate Chain” Prevents Use of Certificate

The Cisco VPN Client does not support the Send CA Certificate Chain option in the Connect Entry. Make sure it is not selected. When this option is selected and a certificate is used, the Cisco VPN Client fails to connect to the secure gateway and logs the IKE log error, `Invalid packet data state (Sender:192)`.

## Mac OS Client Help Inaccessible on Case-Sensitive File System

The VPN client help for Mac OS is inaccessible if one changes the Mac OS file system to be case-sensitive.

The help is accessible if the file system is in its default, case-insensitive format.

## Potential Application Compatibility Issues

You might encounter the following compatibility issues when using the VPN Client with specific applications. Whenever possible, this list describes the circumstances under which an issue might occur and workarounds for potential problems.

### DNS

For DNS resolution, if the domain name is not configured on the network interface, you must enter the fully qualified domain name of the host that needs to be resolved.

### Network Interfaces

- The VPN Client does not support Point-to-Point Protocol over ATM (PPPoA).
- The VPN Client cannot establish tunnels over Token Ring. However, it does not conflict with an installed Token Ring interface.

## Asante FR3004 Cable/DSL Routers Require Asante Firmware Version 2.15 or Later

Versions of the Asante firmware caused a problem with rekeying and keepalives when a VPN Client had an all-or-nothing connection to a VPN Concentrator through an Asante FR3004 Cable/DSL router. Version 2.15 (or later) of the Asante firmware resolves these issues. For more information about Asante cable/DSL routers, see the following Web sites:

- <http://www.asante.com/products>
- [http://www.practicallynetworked.com/pg/router\\_guide\\_index.asp](http://www.practicallynetworked.com/pg/router_guide_index.asp)

## Using Nexland Cable/DSL Routers for Multiple Client Connections

All Nexland Pro routers support passing multiple IPsec sessions through to Cisco VPN 3000 Series Concentrators. To enable this function, the Nexland user must select IPsec Type 2SPI-C on the Nexland options page.

The discontinued Nexland ISB2LAN product correctly handles a single connection, but problems can occur when attempting to make multiple client connections to the same Secure Gateway from behind an ISB2LAN Nexland Cable/DSL router. Nexland has fixed this problem in the Nexland Pro series of routers.

## Cert DN Matching Cannot Match on Email Field EA

You cannot match on the Cert DN field (EA) when using the Peer Cert DN Verification feature because the VPN Concentrator does not assign a value to that field.

## America Online (AOL) Interoperability Issues

### AOL Versions 5.0 and 6.0

The VPN Client supports AOL Version 5.0. AOL Version 6.0 is also supported, with one limitation: when connected, browsing in the network neighborhood is not available.

### AOL Version 7.0

AOL Version 7.0 uses a proprietary heartbeat polling of connected clients. This requires the use of split tunneling to support the polling mechanism. Without split tunneling, AOL disconnects after a period of time between 5 and 30 minutes.

### VPN Client Fails to Connect over Some AOL Dialup Connections

The Cisco VPN Client connecting over an AOL dialup connection fails to complete the connection, particularly when using AOL 7.0 and 8.0

The AOL dialup process uses a fallback method, which, if your initial attempt to connect fails, resorts to a different connection type for the second attempt. This second attempt can sometimes cause AOL to communicate over two PPP adapters (visible in `ipconfig /all` output). When this happens, the VPN Client cannot connect. This is a known issue, and AOL is investigating the problem.

To work around this issue, try to reconnect the dialup connection and try to avoid getting two PPP adapters.

## Browser Interoperability Issues

The following known issues might occur when using the VPN Client with the indicated browser software.

## Entrust Entelligence Issues

The following known issues might occur when using Entrust Entelligence software with the VPN Client.

### Potential Connection Delay

Using the VPN Client with Entrust Entelligence might result in a delay of approximately 30 seconds if you are trying to connect while Entrust is “online” with the CA. This delay varies, depending on your Entrust CA configuration. If the Entrust CA is on the private network, then the chance of Entrust being online are low, since the VPN connection is needed to communicate with the CA.

If you experience this delay, do *one* of the following:

- Wait for the delay to end and proceed with the VPN connection normally.
- Before initiating the VPN Client connection, log out of Entrust. The VPN Client will initiate the Entrust Login Interface with the “work offline” checkbox checked, which alleviates the problem. The easiest way to log out of Entrust is to right-click on the Entrust tray icon (gold key) and select “Log out of Entrust.”

### Entrust Client May Appear Offline

After establishing a VPN connection with Entrust Entelligence certificates, the Entrust client may appear offline. It may appear this way even after the Entrust client has successfully communicated with the Entrust i500 directory.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Once connected, right click on the Entrust tray icon (gold key) and uncheck “Work Offline”. This manually puts Entrust online.

### Renewing Entrust Entelligence Certificate (Key Update) Requires Entrust Version 5.1 SP 3 or Later

Entrust Entelligence certificate renewal (key update) will not work over a VPN Client connection unless Entrust Entelligence version 5.1 SP3 or later is being used. Other Entrust Entelligence operations using older versions work properly.

To work around this issue, do *one* of the following:

- Upgrade to Entrust Entelligence version 5.1 SP3 or later.
- Computers need to have Entrust digital certificates renewed by placing them directly on the network during the renewal period to get updated.

## Accessing Online Glossary Requires Connection to Cisco.com

The Glossary button at the top of all Help screens tries to contact univercd at www.cisco.com (the Cisco documentation site). This connection requires connectivity to Cisco's main web site. If your PC does not have a corporate Internet connection or your firewall blocks access, the following error appears when you attempt to access the Glossary:

“The page cannot be displayed.”

To access the Glossary, you must be connected to www.cisco.com.

## DNS Server on Private Network with Split DNS Causes Problems

When an ISP's DNS server is included in the Split Tunneling Network List and Split DNS Names are configured, all DNS queries to domains other than those in the Split DNS Names list are not resolved.

By definition, split DNS is used so that only certain domains get resolved by corporate DNS servers, while rest go to public (ISP-assigned) DNS servers. To enforce this feature, the VPN Client directs DNS queries that are about hosts on the Split DNS Names list to corporate DNS servers, and discards all DNS queries that are not part of the Split DNS Names list.

The problem occurs when the ISP-assigned DNS servers are in the range of the Split Tunneling Network List. In that case, all DNS queries for non-split-DNS domains are discarded by the VPN Client.

To avoid this problem, remove the ISP-assigned DNS server from the range of the Split Tunneling Network List, or do not configure split DNS.

## No Limit to Size of Log File

When logging is enabled on the VPN Client, all of the log files are placed in the Program Files\Cisco Systems\VPN Client\logs folder with Windows, or the /var/log folder with Mac OS X, and are date and time stamped. There is no limit to the size of the log when logging is enabled. The file continues to grow in size until logging is disabled or the VPN Client program is closed. The log is still available for viewing until the VPN Client program is re-launched, at which time the display on the log tab and log window are cleared. The log file remains on the system and a new log file is created when the VPN Client, with logging enabled, is launched.

## Linksys Wireless AP Cable/DSL Router Version 1.44 or Higher Firmware Requirement

To use the VPN Client behind a Linksys Wireless AP Cable/DSL router model BEFW11S4, the Linksys router must be running version 1.44 or higher firmware. The VPN Client cannot connect when located behind a Linksys Wireless AP Cable/DSL router model BEFW11S4 running version 1.42.7 firmware. The VPN Client may see the prompt for username/password, then it disappears.

## VPN Client GUI Connection History Display Lists Certificate Used

Since Release 4.0.3.C, the VPN Client GUI connection history dialog box displays as the first entry the name of the certificate used for establishing the connection.



## VPN Client cTCP Connection Fails If Checkpoint Client Is Installed

When the Checkpoint VPN-1 Secureremote client is installed with the Release 4.6 or higher VPN Client, and the VPN Client attempts to connect using cTCP, the VPN Client cannot make the connection. Connections do work with UDP, NAT-T, and non-NAT connections.

To make a connection with cTCP when the Checkpoint VPN-1 Secureremote is installed, you must disable the Check Point SecuRemote driver for the Local Area Connection you use.

## Open Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The following lists are sorted by identifier number.



### Note

If you have an account with CCO, you can use Bug Navigator II to find caveats of any severity for any release. To reach Bug Navigator II on CCO, choose Software & Support: Online Technical Support: Software Bug Toolkit or navigate to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

- CSCdt07491

The VPN Client might swap Primary and Secondary WINS received from the Concentrator. In a few cases, the VPN Client receives a Primary and a Secondary WINS server from the Concentrator but swaps them when they are added to the IP Configuration. If this happens, it might cause browsing problems if the Secondary WINS server is not as populated as the Primary. Disconnecting and reconnecting may fix the problem.

- CSCdt07673

When the VPN Client is installed on a Windows 2000 PC with the Efficient Networks NTS EnterNet 300 PPPoE version 1.41 or 1.5c, the following message appears:

“EnterNet could not find the (adapter) for complete pc management NIC (adapter). But it did locate the (adapter) for complete pc management NIC (adapter) - Deterministic Network Enhancer Miniport adapter through which your network server is reachable. Do you want to switch to this adapter?”

Answer Yes to this question. The installation then continues normally.

If the VPN Client is uninstalled, the next time the NTS EnterNet 300 PPPoE version 1.41 is used the message, “EnterNet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No”

Answer Yes to this question. The installation then continues normally.

- CSCdt07787

Problems have occurred when an ISA legacy NIC card (IBM Etherjet 10MB) is used in a PC with PnP OS enabled. The WINS servers did not function correctly when a VPN Client connection was made. This could be an issue with other legacy NIC cards as well.

The end results are that the WINS servers sent from the Secure Gateway cannot be viewed in the Network configuration, and problems with browsing/logon over the VPN connection may occur.

*Workaround:*

Disable PnP OS in the PC's BIOS or statically configure the WINS servers.

- CSCdt13380
 

When you connect the VPN Client to a VPN 3000 Concentrator that issues two DNS servers, both appear under ipconfig /all, but only one appears under the Network settings TCP/IP Properties. DNS server appears to be missing under TCP/IP Properties (Advanced button, DNS TAB). We do not know whether this causes any problems.
- CSCdt56343
 

You might see the following problem on Windows 2000 when you are using the Start Before Logon feature of the VPN Client with third-party dialer. If the third-party dialer does not get set to the foreground when launched, add the following parameter to the vpnclient.ini file in the VPN Client directory (\Program Files\Cisco Systems\VPN Client\Profiles):

```
[main]
TopMostDelay=2500
```

The value is the time in milliseconds that the VPN Client waits for the third party dialer to load before attempting to place it in the foreground. The default time is 1000 milliseconds.

*Workaround:*

For problem dialers/applications, try 2500 milliseconds or greater.
- CSCdu22174
 

SCEP enrollment might fail to complete successfully after the PKI administrator has granted your request.

*Workaround:*

If this happens, delete your failed request and submit a new one. To delete the request, click the Certificate tab, select the failed request, and click Delete on the toolbar. Alternatively, open the Certificates menu and select Delete.
- CSCdu50445
 

The following issue can exist when using the VPN Client Start Before Logon feature with Entrust SignOn. Entrust SignOn is an add-on to the Entrust Entelligence client that allows logging into the Entrust profile and the NT domain from a single login.

The Entrust SignOn GINA dll does not support chaining to other GINA dll files. To make the Entrust SignOn product and the VPN Client with Start Before Logon function properly together, install the VPN Client after Entrust SignOn. The VPN Client replaces the Entrust GINA (etabgin.dll) with its own (csgina.dll).
- CSCdu62275
 

VPN Client and Entrust Entelligence - VPN Connection timeout.

In version 3.1, the potential exists for the VPN Client Connection Manager and the VPN dialer to get out of sync with each other. This occurs only after a VPN Client upgrade on the first time the VPN Client accesses a given Entrust profile. The following sequence outlines how a user could get the connection into this state:

- 
- Step 1** In the VPN dialer, the user clicks Connect.
  - Step 2** Entrust prompts for password and security hash check. The user clicks Yes.
  - Step 3** Entrust prompts for password for cvpnd.exe security access. If the user waits or walks away, the VPN Connection times out in 3 minutes.
  - Step 4** The user returns and enters the Entrust password, then clicks Yes to the security hash check question.
  - Step 5** The VPN connection completes, and data can be passed. The VPN dialer appears as not connected.

**Step 6** Clicking Connect returns, “A connection already exists.” The user clicks Cancel, and the dialer appears connected in the system tray.

The VPN connection can be used as a normal connection.

- CSCdu77405

The message, “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server.” might appear on a PC when Start Before Logon is enabled on the Client and ZoneAlarm is also running. The message appears when the ctrl+alt+del key combination is pressed. This has happened because the Cisco Systems VPN Service has terminated unexpectedly.

*Workaround:*

Logon to the PC with cached credentials, open “Services” in control panel and start the VPN service. A connection to the VPN Concentrator will be possible once the service has started.

- CSCdu81905

When connecting to a VPN 3000 Concentrator over PPPoE using the EnterNet 300 client software from Efficient Networks, Inc., if a firewall is required by the VPN Concentrator, the following message might appear:

“The Client did not match any of the Concentrator's firewall configurations...”

If this message appears, click OK and then click Connect. The connection to the VPN Concentrator then proceeds successfully.

- CSCdu83054

If you make connections from the command line interface, the following problem can occur. When a firewall is required to connect and the firewall fails or is shut down, you do not see any message giving the reason for the lost connection.

- CSCdu86399

If you use the VPN Client with a Digital Certificate and your Client sits behind a Cable/DSL router or some other NAT device, you might not be able to connect to your VPN Gateway device (that is, the VPN 3000 Concentrator). The problem is not with the VPN Client or the Gateway; it is with the Cable/DSL router. When the VPN Client uses a Digital Certificate, it sends the Certificate to the VPN Gateway. Most of the time, the packet with the Certificate is too big for a standard Ethernet frame (1500), so it is fragmented. Many Cable/DSL routers do not transmit fragmented packets, so the connection negotiation fails (IKE negotiation).

This problem might *not* occur if the Digital Certificate you are using is small enough, but this is only in rare cases. This fragmentation problem happens with the D-Link DI-704 and many other Cable/DSL routers on the market. We have been in contact with a few of these vendors to try to resolve the issue.

Testing with the VPN Client Release 3.1 indicates that VPN Client connections using Digital Certificates *can* be made using the following Cable/DSL routers with the following firmware:

Linksys BEFSRxx      v1.39 or v1.40.1

SMC 7004BR Barricade   R1.93e

Nexland Pro400      V1 Rel 3M

NetGear RT314      V3.24(CA.0)

Asante FR3004      V2.15 or later

Others like 3COM 3C510, and D-Link DI-704 either had updated firmware that was tested and failed, or had Beta firmware that was NOT tested because the firmware notes did not indicate a fix specifically for fragmentation.

- CSCdu87521

The following message might appear when a connection using the EnterNet 300 version 1.4 PPPoE software and transferring via FTP:

```
93 09:42:06.020 08/02/01 Sev=Warning/2 IPSEC/0xE3700002  
Function CniInjectSend() failed with an error code of 0xe4510000 (IPSecDrvCB:517)
```

This does not interfere with your connection. You can ignore this message.

- CSCdv40009

When Zone Alarm's Internet setting is set to high and the VPN Concentrator sends a CPP firewall policy that allows inbound traffic on a specific port, the CPP rule takes precedence over the Zone Alarm rule allowing the specified port to be open.

- CSCdv42414

Importing a PKCS12 (\*.p12 or \*.pfx) certificate using the Certificate Manager that has not been password protected will fail with the following error:

“Please make sure your import password and your certificate protection password (if for file based enrollment) are correct and try again.”

*Workaround:*

Get a \*.p12 certificate that has been password protected.

- CSCdv44529

Attempting to install/uninstall Gemplus Workstation version 2.x or earlier while the Cisco VPN Client and its GINA (csgina.dll) is installed will cause the following error, and Gemplus will not install/uninstall:

“A 3rd party GINA has been detected on your system. Please uninstall it before installing this product.”

*Workaround:*

Do *one* of the following:

- Uninstall the VPN Client and reinstall it after Gemplus software.

or

- Use Gemplus version 3.0.30 that no longer installs the gemgina.dll

- CSCdv46591

When a CPP Firewall policy is in place that drops all inbound and outbound traffic and no WINS address is sent to the VPN Client from the 3000 series Concentrator, Start Before Logon fails. If a WINS address is in place, Start Before Logon works fine. Also, if a WINS address is sent and the CPP rule drops all inbound traffic, but allows all outbound traffic, Start Before Logon works fine.

- CSCdv46937

Using the Aladdin “R2” model etoken, certain functions can be performed using the certificate even after the R2 token has been detached from the system (USB port). The VPN Client, for instance, can perform an IKE rekey without the token attached to the system. The reason for this is the design of the “R2” etoken: it does not contain the RSA key functions needed and must upload the private key to the system for these functions.

In contrast, the Aladdin “PRO” etoken must be connected to the USB port during an IKE rekey, otherwise the VPN Client connection terminates. This is Aladdin’s problem; it is not a VPN Client problem.

- CSCdv55730

Using the Solaris VPN Client, some applications are unable to operate properly. A possible indicator of the problem is that a large ping is unable to pass through the VPN Tunnel.

No problem exists when passing large packets using cTcp or normal IPSec. When using IPSec over UDP, Path MTU Discovery problems exist, as a result of which large packets cannot be transmitted.

An MTU issue currently exists with the Solaris VPN Client that causes fragmentation errors that might affect applications passing traffic through the VPN Tunnel.

To identify whether the VPN Client is properly fragmenting packets, use the following commands:

```
ping -n <known good ping target address>
```

```
ping -n -s <known good ping target address> 2500
```

The first command ensures that the target is reachable, and the second determines whether fragmentation is an issue

*Workaround:*

- 
- Step 1** Before opening the tunnel, bring down the MTU of the point-to-point interface to the MTU of the rest of the path to the concentrator (generally 1500). This would allow large packets to pass through, when using IPSec over UDP. No problems exist when using normal IPSec or cTcp.
  - Step 2** Set IP Compression to “LZS” in the VPN Group on the Concentrator. This decreases the size of the encrypted packet and might allow the smaller packet to avoid fragmentation. If you are using NAT, switching the NAT method of the client from cTCP (TunnelingMode=1) to UDP (TunnelingMode=0) might also reduce the size of the packet.
- 

- CSCdv62613

When you have multiple VPN Client connections behind Linksys Cable/DSL router, the following problem can occur. Due to a Linksys problem with firmware versions 1.39 and 1.40.1, making multiple VPN Client connections enabling the feature “Allow IPSec over UDP” (transparent tunneling) may cause data transfer problems.

Allow IPSec over UDP is a VPN Client feature that allows ESP packets to be encapsulated in UDP packets so they traverse firewall and NAT/PAT devices. Some or all of the clients may not be able to send data. This is due to a Linksys port mapping problem, that Linksys has been notified of.

*Workaround:*

Use a newer version of Linksys code (higher than firmware version 1.40.1). If you must use one of the problem versions, do not use the “Allow IPSec over UDP” (transparent tunneling) feature when you have multiple VPN Client connections behind Linksys Cable/DSL router.

- CSCdv67594

The following Microsoft Outlook error might occur when the VPN Client connects or disconnects. This occurs when Microsoft Outlook is installed but not configured.

```
Either there is no default mail client or the current mail client cannot fulfill
the messaging request. Run Microsoft Outlook and set it as the default mail
client.
```

To set Microsoft Outlook as the default mail client, right-click on the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail.

- CSCdv73541

The make module process fails during installation of the VPN Client for Linux.

*Workaround:*

The module build process must use the same configuration information as your running kernel. To work around this problem, do one of the following:

- If you are running the kernels from Red Hat, you must install the corresponding kernel-sources rpm. On a Red Hat system with kernel-sources installed, there is a symlink from `/lib/modules/2.4.2-2/build` to the source directory. The VPN Client looks for this link first, and it should appear as the default value at the kernel source prompt.
- If you are running your own kernel, you must use the build tree from the running kernel to build the VPN Client. Merely unpacking the source code for the version of the kernel you are running is insufficient.

- CSCdw60866

Getting Entrust certificates using SCEP does not get the Root CA certificate. The Entrust CA does not send the whole certificate chain when enrolling with SCEP. Therefore, making a VPN Client connection might require the manual installation of the Root certificate before or after SCEP enrollment. Without the existence of the Root CA certificate, the VPN Client fails to validate the certificate and fails with the following VPN Client event/error messages:

“Get certificate validity failed”

“System Error: Unable to perform validation of certificate <certificate\_name>.”

- CSCdw73886

If an attempt to load the VPN Client is made before the Clients Service loads, the following error occurs: “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPsec server.”

*Workaround:*

Wait until the Service has loaded, then start the VPN Client.

- CSCdx04343

A customer had problems enrolling the Mac OS version of the VPN Client. Following some troublesome attempts at debugging the enrollment of the MacOS VPN Client with a Baltimore CA, it was felt that the Documentation should be improved and the Certificate Manager enhanced.

*Workaround:*

It seems that the critical thing as far as Baltimore is concerned is to put either or both of the challenge phrase (-chall) and the host's FQDN (-dn) in the request. This appears to be similar for the successful SCEP enrolment in a Verisign Onsite PKI. Perhaps there's a case for tweaking the interface a bit, or at least making some notes in the manual!

Just doing `cisco_cert_mgr -U -op enroll` only asks for a Common Name, which is not enough. The request that succeeded on two separate Baltimore installations, one of which had an expired RA certificate, was as follows (switches only shown for brevity):

```
cisco_cert_mgr -U -op enroll -cn -ou -o -c -caurl -cadn -chall -dn
```

The `ou` is required for connecting to a Cisco 3030 VPN Concentrator and is the group name. On almost every attempt, the certificate manager dies after starting to poll the CA, with an error in the log: “Could not get data portion of HTTP request”.

If this happens, it is possible to resume the enrollment with `cisco_cert_mgr -E -op enroll_resume`. The last attempt didn't fail at all though, and the certificate manager kept running until the request was approved, which is how it should behave.

- CSCdx51632

If the computer is powered off or loses power during an MSI installation of the VPN Client, the VPN Client may not be registered in Control Panel, and the following may occur when attempting to reinstall:

- A message may appear stating:  
Deterministic Network Enhancer Add Plugin Failed  
Click the “OK” button.
- Error 1722. There is a problem with this Windows Installer package. A program as part of the setup did not finish as expected. Contact your Support personnel or package vendor. Click the “OK” button.
- Error 1101. Error reading from file `c:\config.msi\laff4.rbs`. Verify that the file exists and you can access it. Click the “OK” button.
- Error 1712. One or more of the files required to restore your computer to its previous state could not be found. Restoration is not possible. Click the “OK” button.

After clearing the last message box, restart MSI installation. It should successfully install the VPN Client.

- CSCdx70223

The VPN Client's `xauth` dialog always stays in the foreground so it doesn't get “lost” (on XP it goes to the background and then jumps forward within seconds). The `xauth` dialog does not have focus, however, and it can be difficult to enter the username/password without first clicking on it with the mouse. This was observed on Windows 2000 and XP.

- CSCdx72463

Installing the VPN Client using the Microsoft Windows Installer (MSI) displays “Time Remaining” for the installation. This time is not very accurate and should be ignored.

- CSCdx77292

Microsoft article Q234859 states that for the resiliency feature to work on Windows 4.0, IE 4.01 sp1 and `shell32.dll` version 4.72.3110.0 or greater must be installed on the computer.

- CSCdx78868

The Microsoft Installer (MSI) resiliency (self healing) feature does not restore all files that are installed with the VPN Client. The files that will be restored are files that are associated with the shortcuts under Start | Program Files | Cisco Systems VPN Client.

- CSCdx81491

An issue can occur when using the Release 4.0 VPN Client with Start Before Logon (SBL), after enabling SBL. The first time you log out of Windows, the VPN Client does not load after you press the CTRL+ALT+DEL key combination at the Windows logon prompt.

*Workaround*

Reboot the PC after enabling Start Before Logon; after a subsequent logout, the VPN Client should operate properly.

- CSCdx88063

When attempting to launch the dialer when the dialer is already running on the logon desktop (due to SBL or SBL and AI), the following error occurs instead of the VPN Client dialer loading.

“Single dialer instance event creation failed with error 5.”

This is most likely to happen when Start Before Logon and Auto Initiate are being used on Windows 2000 or XP.

*Workaround*

This is due to the fact that the VPN Client dialer is already running on the “logon desktop”. Most likely during Windows logon the dialer launched and posted an error, the Windows logon was completed and the error was never closed. To work around this error, do the following:

- 
- Step 1** Press CTRL+ALT+DEL to get to the logon desktop.
  - Step 2** Look for and close any VPN Client error dialogs.
  - Step 3** Press ESC to return to the normal Windows desktop; the VPN Client should load normally.
- 

- CSCdy14218

During installation of the VPN Client on a PC that already has the Enternet v.1.5c or v. 1.5c SP2, the following error might appear:

“SVCHOST.EXE has generated errors and will be closed by Windows.”

*Workaround:*

If this message appears, click OK, then reboot the PC when the VPN Client prompts for the reboot. After this, The message does not reappear and all connections work fine.

- CSCdy50648

InstallShield's “Tuner” application produces warnings and errors when validating the Cisco MSI installation package.

- CSCdy70168

A user with the VPN Client cannot establish an IPSec tunnel to a VPN Concentrator running over an Internet satellite connection.

There are three observed results:

- User is never prompted for XAUTH username and password.
- After successfully authenticating, the user cannot transmit/receive any data.
- After successfully transmitting data for approximately 5 minutes, the VPN session is disconnected regardless of the user activity at the time of disconnect.

This problem occurs only if IPSec over TCP is used.

*Workaround:*

Use IPSec over UDP.



- CSCdz48584

The VPN Client on Windows XP using native XP PPPoE client fails to connect when using IPSec/TCP.

*Workaround:*

Make sure that the Windows XP Internet Connection Firewall is disabled for the PPPoE connection. This feature defaults to enabled when the connection entry is created. To disable it do the following.

- 
- Step 1** Run Control Panel, then click on Network Connections.
- Step 2** Right click on the PPPoE connection entry (may be called “Broadband”) and select “Properties”.
- Step 3** Change to the Advanced Tab and uncheck the “Internet Connection Firewall” option.
- 

- CSCdz56076

Some AOL applications might not be usable while a 4.0 VPN Client connection is active. These include the AOL integrated web browser and some internal links. Using external web browsers and other applications should work over the VPN. These issues were seen most recently using AOL version 7.0 and 8.0.

- CSCdz71367

To connect to a VPN 3000 Concentrator requiring Sygate Personal Firewall, Sygate Personal Firewall Pro, using Are You There (AYT), the version of the firewall must be 5.0, build 1175 or later. The VPN Client might not detect an earlier version of the Sygate Personal Firewall and therefore, a connection will not be allowed.

- CSCdz74310

After upgrading, the VPN Client is unable to connect to the VPN 3000 Concentrator. The ability for the VPN Client to negotiate an AES-192 IKE Proposal has been removed. This change affects all VPN Client versions greater than 3.7.2.

*Workaround*

Reconfigure the VPN Concentrator so that it does not require an AES-192 IKE Proposal for VPN Client connections.

- CSCdz75892

The Equant remote access dialer does not automatically connect the Release 4.0 VPN Client, as it could when using the Release 3.x VPN Client. If you have the Equant dialer configured to establish your VPN connection, the VPN Client appears, but you must manually click Connect to connect. An updated, Cisco-specific .dll file is available from Equant to fix this problem.

- CSCdz87404

The 4.0 VPN Client (on Windows 2000 or Windows XP) connects but is unable to pass data over the VPN tunnel. Viewing the routing table using “route print” at a command prompt shows the default gateway has been modified incorrectly as in the example below.

```
0.0.0.0 255.255.255.255 n.n.n.n n.n.n.n 1
```

Where n.n.n.n is the IP address assigned to the VPN.

*Workaround:*

This is due to a misconfiguration on the VPN3000 at the central site. Make sure that the Group Policy Client Config settings for Split Tunneling Policy are correct. If the group is set to “Only tunnel networks in the list” and the Split Tunneling Network List is the predefined “VPN Client Local LAN” list this problem will occur.

If split tunneling is the desired result, change the Split Tunneling Network List to an appropriate list, otherwise make sure that the Split Tunneling Policy is set to “Tunnel Everything” and check “Allow the networks in the list to bypass the tunnel”. This allows for proper Local LAN functionality.

- CSCea03597

When the VPN Client is installed and Start before Logon is configured, logging into an Active Directory Domain might take a long time, with or without a VPN connection.

This issue occurs under the following conditions:

- The VPN Client is installed on Windows 2000 or Windows XP Professional.
- You have enabled “Start before Logon” in the VPN Client.
- You are logging in to a Windows Active Directory domain (not an NT 4 Domain).

*Workaround:*

This problem occurs because of a fix that was added for CSCdu20804. This fix adds the following parameter to the registry every time Start before Logon is enabled:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetLogon\Parameters
ExpectedDialupDelay
```

Removing “ExpectedDialupDelay” from the registry (then rebooting) should fix the problem with slow logons to an Active Directory Domain.

**Caution**

This procedure contains information about editing the registry. Before you edit the registry, make sure you understand how to restore it if a problem occurs.

**Note**

If you disable, then re-enable Start before Logon, this entry is added again and must be removed.

- CSCea16482

If the Digital Certificate you are using has expired, the Windows VPN Client GUI does not popup with an error message indicating it has expired. The only indication you have is in the log file.

A message does appear if you are using the VPN Client command line - vpnclient.exe

- CSCea17705

If a ZoneLabs product such as ZoneAlarm or ZoneAlarm Pro is installed on the PC and the VPN Client is installed or upgraded, ZoneAlarm blocks the VPN Client service (cvpnd.exe). The VPN Client’s splash screen appears, but the GUI does not. ZoneAlarm does not ask the user whether to allow the VPN Client to access the Internet. Additionally, the following error appears after about two minutes:

“The necessary VPN sub-system is not available. You can not connect to the remote VPN server.”

*Workaround:*

Do the following steps:

- 
- Step 1** Open the ZoneLabs product and select “Program Control”.
- Step 2** Click on the “Programs” Tab
- Step 3** Cisco Systems VPN Client's Access permission is a “?” Click under “Trusted” and select “Allow”. The “?” mark changes change to a check mark.
- Step 4** Reboot the PC.
- Step 5** When the PC boots back up, the client will launch normally.
- 

- CSCea22557

When attempting to open the Mac VPN Client GUI, the application immediately quits. If the ipseclog is running before the GUI client starts, the application quits.

*Workaround*

If the ipseclog is running manually in a terminal window, terminate the log using ctrl-c.

If the GUI client had logging enabled and it quit unexpectedly for any reason, the ipseclog might still be running. In this case, open a terminal window and use “sudo killall -9 ipseclog” to terminate the process.

After the ipseclog has been stopped, the VPN Client should open normally.

- CSCea25682

The following Notification might occur if the Cisco Systems Integrated Client is required to make a connection.

“The Client did not match the firewall configured on the central site VPN device. Cisco Systems Integrated Client should be enabled or installed on your computer.”

When this occurs, the connection is not allowed. If this Notification appears, click Close and attempt to reconnect. If this second attempt to connect fails, reboot the PC. The connection should succeed at this point.

- CSCea27524

This problem has two facets. You cannot select text from the VPN Client log tab, and trying to save the VPN Client log results in an empty (zero byte) file. This problem might occur if the VPN Client logging has been enabled, disabled, or cleared.

*Workaround:*

If the all or part of the log must saved, you can select the text with the mouse or by using CTRL+A, and then copy it using CTRL+C. You can then paste it as usual using CTRL+V in Notepad or your favorite editor.

As an alternative, the VPN Client log files are saved to the directory c:\Program Files\Cisco Systems\VPN Client\Logs by default and can be opened and viewed using a text editor and saved as a different name if needed.

- CSCea29976

After the user enters the username and password, the VPN Client machine might go blank for a moment and then continue. This behavior has not shown any negative effect on the tunnel connection or the user's ability to use the PC.

- CSCea62229  
Using the 4.0 VPN Client with Entrust Entelligence certificates, the “Send CA Certificate Chain” option should be grayed out and unavailable, but it is not.  
*Workaround:*  
Checking the “Send CA Certificate Chain” option when using Entrust Entelligence certificates makes the VPN Client connection fail to complete, leave this option unchecked.
- CSCea63957  
If you uninstall the VPN Client from a Windows 2000 or Windows XP Computer with RASPPPOE, the following message box might appear:  

```
Failed to uninstall the Cisco Network Adaptor.  
Error: 0xe000020b
```

  
Click OK. The Client uninstallation then continues normally.
- CSCea75956  
The following problem has occurred with non-Windows VPN Clients. While connected to the VPN Client, DNS resolution to the internal network works at first but fails later in the connection.  
If the workstation is set to use DHCP and receives a DNS address from the DHCP server, the new DNS overwrites the VPN Concentrator's pushed DNS that had been resolving internal network devices. Once the new DNS has overwritten the Concentrator-pushed DNS, internal devices are no longer resolved properly.  
*Workaround:*  
After connecting to the ISP, record the DNS addresses assigned by the DHCP server and hard code them into the workstation. This prevents the workstation from accepting the DHCP-pushed DNS addresses in the future but still allows resolution when not connected over VPN.  
The drawback of this is that if the ISP changes their DNS server addresses, the user must find out the hard way and hard code these new addresses once more.
- CSCea92185  
The PKCS#10 thumbprint for the certificate request is missing on 4.x VPN Client, so it is impossible for the CA to verify the user's request by comparing the thumbprint.  
*Workaround:*  
Downgrade to 3.6.X VPN Client.
- CSCeb48663  
The ‘vpnclient stat firewall’ command cannot be run while not connected. This command should return the state of the firewall at all times, not just when the VPN Client is connected.
- CSCeb83746  
The following problem occurs when using the VPN Client, Release 4.0 running on MS Windows 2000 or Windows XP. After connecting, a “classfull” route is installed in the routing table, due to not receiving a subnet mask.
- CSCec00525  
IPSec SA rekeying fails on VPN Client 4.0.2A/B. The VPN4.0.2A/B and IPSec SA Lifetime Measurement is configured as Data on the VPN 3000 Concentrator.  
*Workaround:*  
Use Time Lifetime on the VPN 3000 Concentrator.

- CSCec18923  
After the Cisco VPN Client is connected, the PC stops receiving the local multicast traffic. The “Allow Local LAN Access” check box is checked, and the multicast addresses are also included in the bypass list on the VPN 3000 Concentrator.
- CSCec20680  
The ForceNetLogin feature might not work properly with Entrust Intelligence client version 6.1
- CSCec22783  
VPN Client sends the first esp packet after IKE negotiation is successful using an SPI number that doesn't exist. Then the central-site Concentrator sends back a delete notification, which the client ignores because the SPI doesn't actually exist in the VPN Client. This does not affect any functions.
- CSCec30347  
A customer installed an RSA Keon CA server with root and subordinate CA. When we are using the VPN Client, Release 3.1 with the certificates, we can connect to VPN 3000 Concentrator running either 3.x or 4.0.1D (Concentrator code does not matter).  
Once I upgrade the VPN Client to 3.6.x or 4.0.x, I can no longer get a connection to VPN 3000 Concentrator.  
I play around all the settings including “check uncheck CA chain” on the Client end, as well as the Concentrator end, “Certificate Group Matching”, IKE group 1 or group2, no matter what I do, it does not work.  
*Workaround:*  
Downgrade the VPN client to 3.1.
- CSCec47637  
Using VPN Client version is 4.0.1 with a multiple-monitor display enabled on a Windows XP machine, the VPN Client authentication dialog box appears split between the two monitors rather than completely in one side or the other.
- CSCed05004  
With the VPN Client, Release 4.0.x installed on a Windows XP (tablet edition) system, whenever the VPN dialer is opened we get an error “System Error: IPC Socket allocation failed with error ffffffff8h” and then it cannot go out to the DHCP server and get an ip address
- CSCed11256  
When installing a customized VPN Client InstallPath, a pop-up box appears during the installation with the following message:  
Usage:  
VAInstaller i <INF Location> <HardwareID>  
          r <HardwareID>  
          f <HardwareID>  
Options:  
i - installs the Virtual Adapter  
r - removes the Virtual Adapter  
f - finds if the Virtual Adapter in installed  
*Workaround:*  
If the installation path includes \$BASEDIR\Program Files\, then the InstallPath works.

- CSCed90732  
 Windows VPN Client version 4.0.3 fails to enroll with IOS CA server using SCEP. Other devices (PIX, IOS) enroll successfully.  
 The VPN Client does get the CA certificate installed but not the user certificate. The following error results:  

```
error 42: unable to create certificate enrollment request
```

  
 The Client log shows:  

```
Could not find data portion of HTTP response from CEP server. Contact your CA administrator for further instructions.
```

  
*Workaround:*  
 Enroll via a pkcs10 requests.
- CSCee08782  
 Mac OS X VPN Client Release 4.0.3.E and later no longer supports Mac OS X 10.1.5. VPN Client Release 4.0.2.C is the last released client compatible with Mac OS X 10.1.5.  
*Workaround:*  
 Install the Mac OS X VPN Client Release 4.0.2.C.
- CSCee49392  
 Terminating the cvpnd or vpnclient process causes the VPN Client to claim that it is already connected. You should terminate the VPN Client connection only by using the vpnclient disconnect command.  
*Workaround:*  
 Terminate any residual vpnclient and cvpnd processes that might still be running.
- CSCee68280  
 When attempting to tab through the options of a new profile, the Mutual Group Authentication button is never highlighted. It should be highlighted right after the Group Authentication button.
- CSCee74900  
 On a linux multiprocessor kernel the VPN Client seems to pass traffic much slower than on a single processor kernel with the same hardware.  
 In order to work with an SMP kernel the VPN Client was modified in such a way that the performance is lower than the same client run with a single processor kernel.  
*Workaround:*  
 Use a single processor kernel with the VPN Client.
- CSCee93430  
 VPN client fails to connect to Virtual Cluster master real address. Client Firewall is enabled. IPSec/TCP in use.  
*Workaround*  
 Use IPSec/UDP, and Disable the firewall option on the client.

- CSCee95701

If the Microsoft Windows client dns-resolver tries to resolve an unqualified DNS request (for example, a request from client browser for <http://local> [see the scenario that follows]), it takes a long time (more than 15 seconds) to resolve the query.

*Scenario:*

```

DNS-SERVER (zone aa.com)                local DNS-SERVER (zone bb.com)
  |                                       |
VPN-CONCENTRATOR--<INTERNET>--LOCAL-ROUTER---Server(local.bb.com)
  |                                       |
Server(intern.aa.com)                    VPN-Client (split-dns-mode)

```

The delay is introduced, because VPN-client drops A-queries with split-dns suffix(aa.com) when sent to local DNS-Servers.

- CSCef51072

Problem after receiving a Novell log message using Internet Explorer browser proxy. Using the Windows 4.6 VPN Client, the client or service crashes soon after making a successful connection. The last log message from the client is “Novell not installed.”

*Workaround:*

Go into Internet Explorer and uncheck the Proxy Server checkbox found under Internet Options | Connections | LAN Settings.

- CSCeg00709

Entrust certificates that do not expire until 2048 do not work with the VPN Client; it shows the expiry date as 1970. To fix this, the VPN Client needs to support 64-bit time fields.

- CSCeg13025

When using multi-tiered CA between the VPN Client and the IOS, the Client does not process both the x509 certs it has received.

*Workaround*

Make sure that the Client has the certificate chain for the Certificates the IOS device is sending.

- CSCeg24018

We have reproduced this in our lab using latest VPN client 4.0.5C, PIX 6.3.4, and IOS router 12.3(11)T

A Cisco VPN Client cannot connect to a PIX when using a Certificate issued by the Cisco IOS CA server.

In addition, a Cisco VPN Client cannot connect to a router when using a Certificate issued by the Cisco IOS CA server.

However, a PIX and a router using same Certificates can build LAN-to-LAN tunnels to each other.

- CSCeg24804

After making a VPN Client connection with split tunneling, traffic to a local NFS server that bypasses the tunnel does not work properly.

Files may be put onto the server while the tunnel is up, but getting files from the server fails with the following ipsec log message:

```

212    16:05:18.360  11/02/2004  Sev=Info/4IPSEC/0x43700003
Receive: Could not find first fragment; packet dropped (Src:192.168.0.2 Id:29068
Offset:2960)

```

```

213    16:05:18.360  11/02/2004  Sev=Info/4IPSEC/0x43700003

```

```
Receive: Could not find first fragment; packet dropped (Src:192.168.0.2 Id:29068
Offset:1480)
```

- CSCeg32621
 

VPN Client version 3.6.x connecting using IPSec/TCP, large cert, and send chain enabled fails to connect and causes IKE length errors. This occurs under the following conditions: connecting into an ASA device with 2048- or 4096-bit certs, sending chain, and IPSec/TCP

*Workaround*

Use smaller certs, don't send chain, install needed certs on both ends if possible.
- CSCeg36511
 

A VPN Client using large certs (2048 bit keys) and sending the cert chain fails to connect under the following conditions: connecting into a VPN 3000 Concentrator using a 2048 bit cert and with send chain configured.
- CSCeg56330
 

When using “start before logon”, the Cancel connect button does not work.

*Workaround*

Use ctl-alt-del on the PC, login to the machine, then relaunch the VPN Client.
- CSCeg82076
 

When connecting a Windows VPN Client, the pushed browser proxy settings are not applied when working under the following conditions.

When Fast User Switching is involved, the VPN Client attaches itself to the first user to use the VPN Client. If the workstation is then switched to another user and the VPN Client is run, the VPN Client attempts to adjust the registry for the original user to use the Browser Proxy pushed from the VPN Client; this fails.

*Workaround*

Avoid using Fast User Switching or stop the cvpnd service before leaving the previous user:

```
net stop cvpnd (old user)
net start cvpnd (new user)
```

Or reboot the workstation and log in as the new user.
- CSCeh11214
 

Mac OS X VPN Client fails to connect with Certs when Windows Clients connect with the same certs without a problem. A chained Identity Cert is in use on the Concentrator.

*Workaround*

Install an Identity Cert that is not chained.
- CSCeh15956
 

When the VPN Client launches the xauth application while using Radius with Expiry, if you delete the domain name field, the VPN Client might fail.
- CSCeh17548
 

VPN Client fails to connect over dialup with Windows XP. Only Windows XP and dialup exhibit the issue.

*Workaround*

Downgrade to the 4.6.01.0019 VPN Client.



- CSCeh20734

The following program error with dr.watson occurs when toggling back and forth between the simple mode to advanced mode:

```
vpngui.exe has generated errors and will be closed by Windows.  
You will need to restart the program.  
An error log is being created.
```

This symptom occurs on Windows 2000, SP4 with VPN Client release 4.6 (both IS and MSI).

*Workaround:*

Do not toggle back and forth from simple to advanced mode.

- CSCeh21310

Windows XP workstations with the built in firewall turned on seem to cause the VPN Client to disconnect if the KeepAlives are not turned on for the VPN Group or the Confidence Interval is set to 0, the Client cannot rekey properly through the XP built in firewall.

*Workaround*

Enable KeepAlives on the Concentrator with the default 30 second interval, lengthen the period of the IPsec rekey, or disable the built in XP firewall.

Alternatively, in the VPN Client profile, add the keyword "ForceNatT=1".

- CSCeh26526

Windows XP VPN Client disconnects for no reason. The Windows XP Integrated Firewall blocks rekey attempts from the Concentrator to the Client.

*Workaround*

In the VPN Group, turn on IKE Keepalives and set the Confidence Interval to 30 seconds. This is the default for the VPN 300 Concentrator.

Alternatively, configure the Windows XP Firewall to allow traffic from port 500.

- CSCeh54674

Running VPN-Client in a windows environment in combination with NAC, although start-before-logon is configured, logon-scripts might fail.

- CSCeh56322

After making a Windows VPN Client connection, all access to the local DHCP server is lost except for DHCP traffic. SSH, telnet, ping, http... all fail.

On the Windows Virtual Adapter, a route is placed so that DHCP can be renewed locally. This route bypasses the tunnel, but the VPN filter blocks all traffic types except for DHCP. This effectively cuts off all other communications to the DHCP server.

*Workaround*

Use split tunnels and exclude the DHCP server's address from being tunneled. This allows all traffic to the local DHCP server to be bypassed.

- CSCei09677

When running Integrity Desktop v5.1.556.187 and VPN Client v4.6.03.21 on the same Windows machine, both applications function as expected. The VPN Client uninstalls as expected, but the uninstall of Integrity Desktop hangs

- CSCei11378  
When attempting to start the VPN Client log using the GUI, the following error appears in the log:  
Error 47: Failed to load ipseclog.exe  
This affects all Mac OS X versions.  
*Workaround:*  
Click the Enable log button a second time to start the log.
- CSCei30835  
In rare situations, the GUI stops responding. Wireless connectivity is lost and immediately regained. VPN service is properly disconnect before the system goes into standby mode.  
*Workaround:*  
Use Task Manager to stop the GUI.
- CSCei48783  
When running Classic with a VPN Client, a ping over 150 bytes or so causes a kernel panic when executed in either Classic or OS X. This “may” only be an ICMP issue. Apple no longer supports classic on OS X 10.4 and future releases.
- CSCsa74320  
During a VPN connection a bluescreen or lockup of the Windows XP/2000 machine causes the profiles to be corrupted. All of the profiles contain only the following after this occurs:  

```
[main]
UserPassword=
enc_UserPassword=
```
- CSCsb24801  
A Cisco VPN Client, Releases 3.6.x and 4.6.x, might crash a Win 2000 or Win XP laptop when remote access connection type is Wireless - Wi-Fi and Ethernet.  
When trying to change from Wi-Fi connection to the Wireless connection and visa versa, the operating system crashes. The user receives the error message, “unexpected kernel mode trap” and must restart the host. This does not happen if VPN Client is not installed.  
*Workaround:*  
Disable the current connection type first, then enable the second one and restart the host.
- CSCsb68239  
Using Cisco VPN Client with Entrust and Rainbow/Safenet iKey 2032 tokens, providing a bad password for the authentication can trigger the locking of the token/smart card.  
The following message appears in the VPN Client logs:  

```
"IKMPLLogin" returned error = (-160) Incorrect password supplied."
```
- CSCsb71158  
The following scenario occurred with a Cisco VPN Client on Windows XP, connecting to Cisco 7200 router acting as an IPSec Gateway. Pings whose IP size is less than or equal to 1300 bytes are successful and without fragmentation; Pings whose IP size is within the range 1301 bytes through 1320 bytes are successful, but the Windows system fragment all outgoing packets. Pings whose IP size is greater than or equal to 1321 bytes are unsuccessful.

- CSCsb73788
 

A Macintosh VPN client connected to a VPN Concentrator cannot access some private networks; that is, networks behind the VPN Concentrator.

This problem occurs when the machine running the VPN Client is located in a network that overlaps with the private network that the VPN client is trying to access. This happens regardless of whether local LAN access is permitted on the VPN client.

As an example, if the machine running the VPN client obtains the address 192.168.1.10/24 via DHCP, and the host it is trying to access is located in the private network 192.168.1.0/24, communication fails.

This scenario is possible in places like hotels that offer high-speed Internet access, especially if the hotel chooses to use a big IP network for its internal network; for example, 10.0.0.0/8.
- CSCsb74361
 

When using tunnel-default-gateway, VPN Client to Client communication does not work unless the packet is first sent from the client that connected first to the client that connected afterwards.
- CSCsb75929
 

When an MSI installation is automated through Active Directory, the software gets installed in a system context and the virtual adapter MTU is not set.
- CSCsb93222
 

When using the Server version of OS X 10.4 and the VPN Client, the server has a kernel panic.

This issue is caused by the AFP Service running on the server conflicting with the VPN Client. It is similar to an OS X 10.4 workstation AFP conflict that was resolved. Now the Server version on OS X 10.4 needs similar attention.

*Workaround*

Turn off the AFP Service on the server.
- CSCsc20169
 

Need to document a new feature that allows the installation of the Windows VPN Client without installing a new vsdata.dll file.

*Workaround*

See the [Documentation Changes, page 34](#) for this documentation.
- CSCsc25862
 

When exporting certificates with the VPN Client from inside the Cisco store, the exported file isn't a pkcs#12 format but a proprietary one. This should be mentioned in documentation. Certificates are stored in the Cisco certificate store.
- CSCsc33384
 

Enrollment requests generated by the VPN Client have an associated sha1 thumbprint. This thumbprint does not match that generated by an external authority (openssl).
- CSCsc48265
 

When using Exclude Local LAN and other excluded networks with the VPN Client, the Split DNS feature is not available. Split DNS works only when specific networks are tunneled, not excluded.

*Workaround*

Use split tunnels instead of excluded in order to use the Split DNS feature.

- CSCsc48282

Feature to add more than one domain to the VPN Client workstation search list during a connection. Currently, on the Client, the pushed Default Domain Name is added to the search list.

*Workaround*

Use Split DNS with the AppendSplitDNSSuffix=1 keyword in the vpnclient.ini file under the [DNS] section.

- CSCsc70505

Installing the VPN Client does not produce an install shield log file. This means I cannot uninstall the VPN Client on a Tablet PC. When the customer tries to install another VPN Client, the installation hangs.

- CSCsc85177

VPN Client virtual adapter routing is corrupted by ICMP redirect. A VPN Client connection connects successfully and passes traffic but later dies due to a loss of connection with the gateway even when traffic was passing.

If the workstation is on a network with more than one gateway, it could be receiving an ICMP redirect from the default gateway that is directing traffic for the Concentrator through a different gateway. When this ICMP redirect later expires, the VPN Client loses connectivity with the Concentrator, and the connection is lost.

*Workaround*

Disable ICMP redirects on the workstation.

Windows example in the registry:

```
[HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\TCP\IP\PARAMETERS]
"ENABLEICMPREDIRECTS"=DWORD:00000000
```

- CSCsc88145

When a Mac has firewire using TCP/IP, the VPN Client fails to behave properly. Unplugging the firewire resolves the issue. Firewire TCP/IP seems to have an MTU of 2030.

- CSCsd01896

The VPN Client for Windows does not install the MSI French help file.

*Workaround*

Create a custom web page and point the VPN Client at the online web page rather the Cisco help file using the 4.7.00.0533 Windows VPN Client or higher.

The following keyword in the vpnclient.ini file allows the VPN Client to direct help to an online web server:

```
[GUI]
HelpURL=<URL for help files>
```

For example:

```
HelpURL=http://www.cisco.com
```

Do NOT put quotes around the url.

The following appears in the VPN Client log with the appropriate custom url:

```
1      11:38:49.710  07/14/05  Sev=Debug/7GUI/0x63B0000C
```

The value for vpnclient.ini variable HelpURL is C:\Program Files\Cisco Systems\VPN Client\pophelp.html.

- CSCsd07876

The software license presented during client installation was not updated when the hardcopy software license was revised. Some terms of licensing have been changed.

- CSCsd17584

When using the CLI to disconnect the Mac OS X VPN Client, the command produces the following output:

“The VPN sub-system is busy or has failed.”

This appears only when using the “vpnclient disconnect” CLI command and does properly disconnect the VPN Client without any adverse effects.

- CSCsd17602

When attempting a large NFS transfer through the Linux VPN Client, the workstation freezes or crashes. This appears only in kernel versions above 2.6.9 that use a 4K kernel stack size. RedHat installs with this kernel size by default above 2.6.9.

*Workaround*

Reinstall the kernel with an 8K kernel stack size.

- CSCsd18619

The Unix version of VPN Client has world-writable configuration files.

- CSCsd25779

VPN Client fails during phase1 negotiation if using USB Token with ePass1000 for certificate storage, even when the root cert is imported to MS or Cisco store. This happens under the following conditions:

- USB Token with ePass1000
- VPN Client 4.7 and 4.8

*Workaround*

Downgrade to 4.6 or earlier version.

- CSCsd47428

VPN Client Releases 4.7 and 4.8 (both MSI and IS) for Windows freeze during uninstallation. This happens under the following conditions:

- NAC is enabled at the VPN3000 for the user's usergroup
- Client establishes connection to VPN3000 and then disconnects from VPN3000
- User does not reboot the PC since the last connection to the VPN3000 was made
- User starts the uninstall, PC freezes during uninstall
- PC can be rebooted only via hard reset after freezing.

If NAC was not enabled, uninstall goes smoothly. If PC is rebooted after disconnecting from the VPN 3000 Concentrator, uninstall goes smoothly.

*Workaround*

Reboot before uninstall or make sure no connection attempt was made to the VPN 3000 since last reboot.

This workaround *does not* apply when using the AutoUpdate function, because the AutoUpdate starts the uninstall process right after disconnecting from VPN3000.

IPSec over UDP works fine. This problem is limited to using IPSec over TCP or straight IPSec.

- CSCsd51126

VPN Client connections fail over PPP on the Intel platform with a “mismatch length” error in the vpnclient log. PPC platforms still work fine.

- CSCsd51157

Using Mac OS X 10.4 and PPP, the GUI does not launch and the CLI does not connect.




---

**Note** 10.4 introduced issues that the Apple is unable to advise us upon.

---

*Workaround*

Restart the VPN Service after PPP has been started.

```
/System/Library/StartupItems/CiscoVPN/CiscoVPN stop
/System/Library/StartupItems/CiscoVPN/CiscoVPN start
```

- CSCsd62216

When the “minimize upon connect” option is selected the VPN Client minimizes for a fraction of a second, but immediately thereafter the window pops up again. This happens only when a Banner is being pushed down from the VPN Group.

*Workaround*

Remove the banner from the VPN Group.

- CSCsd76149

When enrolling online using the 4.7.00.0533 VPN Client or higher, the Root CA is not imported when using SCEP and a subordinate CA.

The 4.6.04.0043 VPN Client behaves properly and imports the Root CA with the same test.

The Root CA is imported properly when enrolling directly with the CA Server.

*Workaround*

Import the Root CA manually or have it imported with the installation of the VPN Client using the “rootcert” method described with Hybrid Authentication in the User Manual.

- CSCsd84461

When Using VPN Client, version 4.8, attempting to use IP communicator to talk to CME results in One/No way audio issues. Sometimes you get audio for the first few seconds and then nothing. If you put on hold and resume, you get the same results.

I am not sure if this affects Call Manager as well, or if it is Just CME. It is a VPN Client issue, so I do think it may affect CCM as well as CCME. This is a duplicate of CSCsd69887.

*Workaround*

Using VPN Client 4.7.00.0533 works every time.

- CSCsd86776

When you verify a certificate selected in the VPN Client under “Certificates” and click on verify, you get an error:

```
Error 32: Unable to verify certificate "....."
The selected certificate was signed by a CA whose certificate validity is longer than
year 2099.
```

*Workaround*

Use a CA with shorter lifetime certificate.

- CSCsd94655

The installation scripts for the Linux VPN Client do not set the setuid flag for the cvpnd binary in /opt/cisco-vpnclient/bin.

The “chgrp” command, part of the “coreutils” package that ships with FC5 behaves in a different way from previous versions. When running chgrp to change the group ownership of a setuid file, the setuid flag is turned off during the process of setting the group ownership. The install script uses the chgrp command on this file *after* having first flipped on the setuid flag, turning it off again before completion.

*Workaround*

Manually set the setuid flag on cvpnd by changing into the /opt/cisco-vpnclient/bin directory and issuing the following command:

```
chmod 4111 cvpnd
```

- CSCse06513

Cisco VPN Client fails to select one of the certificates when multiple matching certificates are available.

The customer is using following smart card/token:

- The USB Token:

The USB token contains a Schlumberger FIPS Level-2 smart card that is used to store user credentials.

- Smart Card

PS Card is based on Java card that supports RSA 2048-bit on-board key generation. It is 64KB in size. The manufacturer of our smart card is Oberthur and Axalto.

The smart card readers we are using are as follows:

- SCM 331 (USB)
- SCM 201 (PCMCIA)
- Gem 430 (USB)
- PCI GemCore Based Smart Card Controller

- CSCse18195

On a Microsoft XP computer, the behavior of netsh is not the same with and without the Cisco VPN Client installed. This issue begins with the 4.7.00.0533 VPN Client release.

When the Cisco VPN Client is installed, if we do the following, the parameters from the file “file-name” are not processed:

1. netsh interface ip dump > file-name
2. Change some parameters using netsh
3. Revert to the first conf with netsh -f file-name

*Workaround*

Revert to the 4.6.04.0043 VPN Client version.

- CSCse19083

Windows VPN Clients version 4.6 and above experience performance issues with Viack's Via 3 conferencing software. Either the VPN Client or the conferencing software functions fine on its own. However, if any appreciable amount of traffic is sent over the VPN Client tunnel when the conferencing software is in use, a large CPU spike occurs (90% +), and the audio feed to the computer running the VPN Client cuts out completely. We have observed the following behavior during this problem:

- Once the problem occurs, the host on the computer running the VPN Client can speak and be heard by the other participants but cannot hear them.
- Although sending of the VPN traffic causes a high CPU spike, the problem persists even after the VPN traffic stops and the CPU returns to nominal (0-20%) levels. It appears to be an interoperability issue that completely knocks out the audio drivers
- There is no apparent way to recover other than to leave and rejoin the conference (that is, muting the audio and unmuting, etc., either globally or from the conference software has no effect). Eventually even this has no effect and the only fix is to reboot the affected computer.

The issue appears to be hardware and/or software dependent - it can be reproduced reliably by computers using a specific image on Dell Latitude C400 and other models but is not seen on various IBM Thinkpad laptops. This issue has been observed only with VPN Clients 4.6 and above. Earlier VPN Clients do not experience this issue.

*Workaround*

No reliable workaround. Leaving then rejoining the conference will sometimes fix the issue, but not consistently.

- CSCse24562

When Split DNS is configured for the VPN Client connection, nslookup fails to resolve properly. The nslookup feature is not supported with Split DNS.

- CSCse31161

After a vpn session is connected between 30 seconds and one hour, a blue screen of death occurs. The conditions are as follows:

- A Microsoft OS is installed with the Cisco vpn client and Trend Micro Office Scan version 7.3.
- The Trend Micro FW is activated (the VPN build in FW is deactivated)
- The vpn client is launched and the session gets connected.



- CSCse31399
 

After returning a workstation from sleep that had an active VPN Client connection using an external Certificate device, the VPN Client does not reconnect using the Certificate.

The VPN Client reloads the Certificate Store only when launched and could not find the original Certificate.

*Workaround*

Close and reopen the VPN Client connection after returning from sleep.
- CSCse39772
 

After unzipping the client and running “vpnclient\_setup.msi” from either the desktop or some other location, the VPN Client fails to install because it is unable to copy files into the temp directory.

*Workaround*

Do the following:

  1. Run “vpnclient\_setup.exe”, instead of the .msi file.
  2. Disable UAC
- CSCse48101
 

The Mac VPN Client does not launch anything with the “Help” if Internet Explorer is not installed. Internet Explorer is currently required in order to use online help for the Mac VPN Client.

*Workaround*

Install Internet Explorer for Mac.
- CSCse51257
 

Cisco VPN 4.8.01.0300 Client receives an Access Denied error during install. Using the Windows MSI package, the error occurs right after the DNE package finishes. The process that fails is:

```
CreateDeviceInfo error: Access is denied.
```

It occurs only in an environment where the user is not a member of the Local Administrator group.
- CSCse55128
 

The VPN Client does not apply proxy settings to the browser. this problem occurs only when the “Start before Logon” option is enabled on the VPN Client under Options > Windows Logon Properties

The Proxy settings are being pushed to the VPN Client, as shown in the Client logs. The Client log also shows the following message:

```
50      11:05:27.718  06/16/06  Sev=Warning/3    IKE/0xA300006D
Failed to Apply Browser Proxy Settings to local Browsers.
```
- CSCse56229
 

While deleting profiles using the Windows GUI, the VPN Client crashes. This does not occur with 4.7.00.0533 and below.

*Workaround*

Restart the VPN Client.
- CSCtr23741
 

The VPN Client fails when “Back to my Mac” is enabled.

*Workaround*

Switch off “Back to my Mac” before connecting to the VPN. When the VPN is disconnected, “Back to my Mac” can be re-enabled.

## Resolved Caveats in VPN Client for Mac OS X, Release 4.9.00.0050

The VPN Client for Mac OS X, Release 4.9.00.0050, resolves the following caveat.

- CSCsb80109  
After uninstalling the Mac OS X VPN Client, the next installation claims that it is an “Upgrade”.
- CSCsc29691  
After installing the Mac OS X VPN Client successfully, the VPN Client cannot be launched from either the GUI or CLI. A /tmp directory must exist before the installation of the VPN Client. This directory is automatically created by the OS but might have been deleted by the user.
- CSCsc79998  
After upgrading from the 4.7.00.0510 VPN Client for Mac OS X 10.4, the contents of the /opt directory have been erased. This happens only when overwriting the previous 4.7.00.0510 VPN Client with the 4.8.00.0490 VPN Client. Mac OS X 10.3 is not affected by this issue.

## Documentation Updates

The following VPN Client documentation was updated for Release 4.6 and has not changed for Release 4.7 through 4.9. The following section contains changes to apply to these documents. These documents contain information for all platforms on which the VPN Client runs:

- *Cisco VPN Client Administrator Guide, Release 4.6*
- *Cisco VPN Client User Guide for Windows, Release 4.6*
- *Cisco VPN Client User Guide for Mac OS X, Release 4.6*
- *Cisco VPN Client User Guide for Linux and Solaris, Release 4.6*

When using this documentation, please take into account the following global changes:

- VPN Client for Mac OS X, Release 4.9.00.0050 is the first version that supports both the Power PPC (PPC) and Intel processors. This release for Mac OS X supports only OS X 1.4 and 0.5. It does not support earlier and later releases.
- VPN Client does not support Windows NT, 98, and ME.

## Documentation Changes

The changes in the following sections apply to the *VPN Client Administrator’s Guide*.

## Correcting the Obsolete Filename `vpnclient_en_msi`

Make the following change to the description of MSI installation, right below the “Installing the VPN Client Using the Transform” section. Replace the obsolete file name “`vpnclient_en_msi`” with “`vpnclient_setup.msi`”.

## Using MSI to Install the Windows VPN Client without Stateful Firewall


Some third party applications and virus checkers conflict with the VPN Client's Stateful Firewall (`vsdata.dll` file). To avoid these conflicts, you can install the VPN Client without a new `vsdata.dll` file. Any previous `vsdata.dll` file are left alone, which allows the Stateful Firewall to operate normally. This change pertains only to the Windows version of the VPN Client.

If the VPN Client is installed with the following transform and there is NOT a `vsdata.dll` file already on the workstation, the Stateful Firewall option is disabled. The pulldown option for the Stateful Firewall is removed during the installation. The VPN Client downloads include the file `novsdata.zip`, which includes the transform (`novsdata.mst`) for this installation.

The contents of the `novsdata.zip` file are as follows:

- README
- `novsdata.bat`
- `novsdata.mst`

To use the `novsdata.mst` transform, do the following steps:

- 
- Step 1** Uninstall the Cisco Systems VPN Client if it is installed.
- Step 2** If desired, delete the current “`vsdata.dll`” file from the workstation.
- 
-  **Caution** Do not delete the current `vsdata.dll` file if you are using a third-party Zone Labs firewall.
- 
- Step 3** Modify the `novsdata.bat` file with any other transforms used to customize the VPN Client installation. For instance:
- ```
msiexec.exe /I vpnclient_setup.msi TRANSFORMS=novsdata.mst;myCompanyLogos.mst
```
- Step 4** Unzip the latest VPN Client installation package into a folder, but do not execute the installation.
- Step 5** Place the `novsdata.bat` and `novsdata.mst`, as well as any other custom `mst` files, into the folder used in step 4.
- Step 6** Execute the `novsdata.bat` file to install the VPN Client with the applied `msi` transforms.
- 

## Using InstallShield to Install the Windows VPN Client without Stateful Firewall

The VPN Client, Release 4.7, lets you use InstallShield to disable the Stateful Firewall feature. Make the following documentation change to the *VPN Client Administrator's Guide* under the “Customizing the VPN Client Software” section.

Add the following keyword to the example and `oem.ini` chart under the [Main] section:

```
DisableFirewallInstall=0/1
```

When this variable is set to 1, the Stateful Firewall feature of the VPN Client is disabled. The default value is 0, which allows the use of the Stateful Firewall feature. This flag works only if a vsdata.dll file is not present on the workstation during installation.

## Certificates Exported from Cisco Certificate Store Are in Proprietary Format

When exporting certificates with the VPN Client from inside the Cisco store, the exported file is not a pkcs#12 format, but a proprietary one. Certificates are stored in the Cisco certificate store.

## Related Documentation

- *VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.1*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management, Release 4.1*
- *VPN 3000 Series Concentrator Getting Started, Release 4.1*

---

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2000-2011 Cisco Systems, Inc. All rights reserved.