



Release Notes for VPN Client, Release 4.6.00 through 4.6.04

Updated May 22, 2011

These release notes support Cisco VPN Client software Release 4.6.00 through 4.6.04 on Windows, Macintosh, Linux, and Solaris. Release 4.6.00.0045 is the first VPN Client 4.6 release. Please refer to [About Version Numbers, page 7](#) for information about the new version numbering scheme.

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.

Contents

[Introduction, page 2](#)

[System Requirements, page 2](#)

[Installation Notes, page 4](#)

[New Features in Release 4.6.x, page 7](#)



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

Copyright © 2009 Cisco Systems, Inc. All rights reserved.

[Usage Notes, page 15](#)

[Open Caveats, page 36](#)

[Resolved Caveats, page 60](#)

[Documentation Updates, page 81](#)

[Related Documentation, page 82](#)

Introduction

The VPN Client is an application that runs on a Microsoft® Windows®-based PC, a Sun ultraSPARC workstations, a Linux desktop, or 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 Windows* or *Cisco VPN Client User Guide for Mac OS X*, as appropriate for your platform, 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 indicates the system requirements to install the VPN Client on each of the supported platforms.

Computer	Operating System	Requirements
Computer with a Pentium [®] -class processor or greater	<ul style="list-style-type: none"> • Windows 2000 • Windows XP 	<ul style="list-style-type: none"> • Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.) • 50 MB hard disk space. • RAM: <ul style="list-style-type: none"> – 128 MB for Windows XP (256 MB recommended) – 64 MB for Windows 2000 (128 MB recommended) –
Computer with and Intel x86 processor	RedHat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later Note The VPN Client does not support SMP (multiprocessor) or 64-bit processor kernels.	<ul style="list-style-type: none"> • 32 MB Ram • 50 MB hard disk space
Sun UltraSPARC computer	32-bit or 64-bit Solaris kernel OS Version 2.6 or later	<ul style="list-style-type: none"> • 32 MB Ram • 50 MB hard disk space
Macintosh computer	Mac OS X, Version 10.2.0 or later	<ul style="list-style-type: none"> • 50 MB hard disk space • PPC only. None of the Release 4.6.x versions supports Mac OS X on Intel processors.

**Note**

VPN Client does not support Windows NT, 98, and ME.

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

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

Installation Notes

The following tables list the files included in each release:

vpnclient-win-msi-4.6.00.0049-k9.zip	Windows client MSI installer
vpnclient-win-is-4.6.00.0045-k9.zip	Windows client IS installer
vpnclient-darwin-4.6.00.0045-GUI-k9.dmg	Mac OS X installer
vpnclient-linux-4.6.00.0045-k9.tar.gz	Linux package
vpnclient-solaris-4.6.00.0045-k9.tar.Z	Solaris package
vpn3000-4.1.6.bin	VPN 30xx Concentrator code
vpn3005-4.1.6.bin	VPN 3005 Concentrator code
update-4.6.00.0045.zip	VPN Client AutoUpdate package

Because of platform differences, the installation instructions for Windows and non-Windows platforms also differ.

- Refer to the *Cisco VPN Client User Guide for Windows*, Chapter 2, for complete installation instructions for Windows users.
- Refer to the *Cisco VPN Client User Guide for Mac OS X*, Chapter 2, for complete installation information for those platforms.

The following notes are important for users who are upgrading to Windows XP and users who want to downgrade to an earlier version of the VPN Client software.

Installation Notes - Windows Platforms

Release 4.6 includes the following installation considerations for Windows users:

Installing the VPN Client Software Using InstallShield

Installing the VPN Client software on Windows 2000 or Windows XP with InstallShield requires Administrator privileges. If you do not have Administrator privileges, you must have someone who has Administrator privileges install the product for you.

**Note**

The VPN Client Installer does not allow installations from a network drive.

Installing the VPN Client Software Using the MSI Installer

**Note**

The Windows MSI installation package was first released with version number 4.6.00.0049. No other packages were released from build number 4.6.00.0049.

If you are using the MSI installer, you must have Windows NT-based products such as Windows 2000 or XP. Installing with MSI also requires Administrator privileges.

When installing the Windows MSI installation package, the user must manually uninstall the previous VPN Client if it is older than version 4.6. The version 4.6 MSI installer does not detect older versions, and the installer will attempt to install before aborting gracefully. Once a version 4.6 MSI package has been installed, future client versions will be able to detect the existing version 4.6 installation and automatically begin the uninstallation process.

**Note**

Windows Installer 2.0 must be installed on Windows 2000 before configuring the PC for a Restricted User with Elevated Privileges.

Installation Notes - Solaris Platforms

The following sections describe actions you must take when installing the VPN Client on a Solaris platform.

Uninstall an Older VPN Client If Present on a Solaris Platform

If you have a previous version of the VPN Client running under Solaris, you *must* uninstall the older VPN Client before installing a new VPN Client. You are not required to uninstall an old VPN Client, if one is present, *before* installing a new VPN Client for Linux or Mac OS X.

Refer to the *Cisco VPN Client User Guide for Linux, Solaris, and Mac OS X*, Chapter 2, for complete uninstallation information.

Disable the ipfilter Firewall Kernel Module Before Installing the VPN Client on a Solaris Platform

If you have an IP firewall installed on your workstation, the reboot after installation of the VPN Client takes an inordinate amount of time. This is caused by a conflict between the `vpnclient` kernel module `cipsec` and the `ipfilter` firewall module. To work around this issue, disable the `ipfilter` firewall kernel module before you install the VPN Client.

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, and
- 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)
 - Entrust Technologies (www.entrust.com)

- Netscape (www.netscape.com)
- Verisign, Inc. (www.verisign.com)
- Microsoft Certificate Services — Windows 2000
- A digital certificate stored on a smart card. The VPN Client supports smart cards via the MS CAPI Interface.

New Features in Release 4.6.x

These Release Notes cover several releases in the 4.6.x sequence. Some of these releases offer new features, as detailed in the following sections.

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, 4.6.00.0045 represents feature release 4.6, build 45.

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

These release notes refer to the VPN Client 4.6 software generically where appropriate, and more specifically where necessary to differentiate between patch releases.

New Features in Release 4.6.03.190 (Linux)

This release is a Beta for the VPN Client installed on biarch¹ Linux systems for x86_64 platforms.

1.biarch = 64-bit kernel that allows execution of 32-bit applications.

This release of the VPN Client is NOT compatible with pure 64-bit operating systems.

The VPN Client operates on both 32-bit i386 and biarch x86_64 operating systems.

On i386 32-bit operating systems, this release is not considered a Beta.

The VPN Client now requires GLIBC_2.2 and libstdc++.so.5. Distributions like RedHat 9 and SuSe 9 comply with these requirements.

New Feature in Release 4.6.03.160 (Mac OS X)

This is the first Cisco VPN Client version to support Mac OS X 10.4, but only with single processors. Do not use this version with dual processor platforms running Mac OS X 10.4. Dual processor platforms running Mac OS X 10.2.x through 10.3.x can use this version.

New Feature in Release 4.6.2.0011 for Windows

Release 4.6.2.0011 introduced a feature that lets the administrator configure a user's system to eliminate pop-up messages for an always-up VPN connection.

AutoInitiation Enhancement for Windows VPN Client

With this enhanced AutoInitiation feature configured, AutoInitiation with the Windows VPN Client does not prompt the user about whether to suspend the service. The result is a "transparent" Client that only has the VPN lock in the icon tray when using AutoInitiation. Eliminating the pop-up prompts means that the user does not have the option to suspend the service, because suspending might bypass their security.

New Features in Release 4.6.02.0030 and 4.6.03.190 for Linux

The VPN Client for Linux, Release 4.6.02.0030, supports the following feature.

Support for Solaris 10

The VPN Client for Linux, Release 4.6.02.0030 officially supports Solaris 10.

Firewall Configuration for the VPN Client for Linux with Virtual Adapter

Cisco has designed the following firewall configuration for the VPN Client for Linux that works with the Virtual Adapter. The Virtual Adapter was introduced with the 4.6.02.0030 Linux release. This firewall blocks all traffic on eth0, except for tunneled traffic.

Firewall configuration written by Cisco Systems

```
# Designed for the Linux VPN Client 4.6.02.0030 and 4.6.03.0190
Virtual Adapter
```

```
# Blocks ALL traffic on eth0 except for tunneled traffic
```

```
*filter
```

```
:INPUT ACCEPT [0:0]
```

```
:FORWARD ACCEPT [0:0]
```

```
:OUTPUT ACCEPT [0:0]
```

```
# Allow all traffic in both directions through the VA adapter
```

```
-A INPUT -i cipsec0 -j ACCEPT
```

```
-A OUTPUT -o cipsec0 -j ACCEPT
```

```
# Accept all encrypted VPN Client traffic in either direction on eth0
```

```
-A INPUT -i eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j
ACCEPT
```

```
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 500 -d 0/0 --dport 500 -j
ACCEPT
```

```
-A INPUT -i eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j
ACCEPT
```

```
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 4500 -d 0/0 --dport 4500 -j
ACCEPT
```

```
-A OUTPUT -o eth0 -p udp -s 0/0 --sport 1024: -d 0/0 --dport 29747 -j
ACCEPT
```

```
# Block all other traffic in either direction on eth0
```

```
-A INPUT -i eth0 -j REJECT
```

```
-A OUTPUT -o eth0 -j REJECT  
COMMIT
```

New Features in Release 4.6.00

Release 4.6.00 of the VPN Client software includes the following new features.

- Mutual Group Authentication
- Auto Update (Windows 2000 and Windows XP only)
- Browser Proxy Config (Internet Explorer for Windows only)
- Client API support (all platforms except Solaris)
- Connect on Open (Windows and Macintosh)
- Section 508 Accessibility Compliance (Windows)

Mutual Group Authentication

Group Authentication is a method that uses pre-shared keys for mutual authentication. In this method, the VPN Client and the VPN central-site device use a group name and password to validate the connection. This is a symmetrical form of authentication since both sides use the same authentication method during their negotiations.

Mutual group authentication is asymmetrical in that each side uses a different method to authenticate the other while establishing a secure tunnel to form the basis for group authentication. In this method, authentication happens in two stages. During the first stage, the VPN central-site device authenticates itself using public-key techniques (digital signature) and the two sides negotiate to establish a secure channel for communication. During the second stage, the actual authentication of the VPN Client user by the central-site VPN device takes place. Since this approach does not use pre-shared keys for peer authentication, it provides greater security than group authentication alone, as it is not vulnerable to a man-in-the-middle attack.

To use mutual group authentication, the remote user's VPN Client system must have a root certificate installed. If needed, you can install a root certificate automatically by placing it on the VPN Client system during installation. The certificate must be in a file named rootcert, with no extension, and must be placed in the installation directory for the remote user's VPN Client system.

For more information on mutual group authentication, see the *VPN Client Administrator Guide*, Chapter 1.

You must configure both the VPN Client and the VPN Concentrator to allow mutual group authentication (Hybrid mode). Ensure that the Certificate Authority being used on both the VPN Client and the VPN Concentrator is the same. Configure the VPN Concentrator in a similar fashion to the use of User Certificates.

1. Select an IKE Proposal that allows HYBRID mode authentication such as those listed in Table 8-3 of the *VPN Client Administrator's Guide*. HYBRID-AES256-SHA-RSA for example.
2. Configure an IPSec SA to use the appropriate Identity Certificate to be authenticated with the CA certificate of the VPN Client. If certificates have not yet been obtained for the VPN Concentrator, please refer to the *VPN 3000 Series Concentrator Reference Volume I: Configuration Release 4.1*.
3. Configure a VPN Group to use the new IPSec SA from step 2. The VPN Clients under test for Mutual Group Authentication will be connecting to this group.

Automatic Updates

In an automatic update, the VPN Client downloads a new version of the software and installs all related components automatically for users. This feature also allows the administrator to distribute and update profiles automatically.

Once Windows VPN Client version 4.6.00 has been installed, only the VPN Concentrator and Web server need be configured to initiate Automatic Updates of the Client. Please refer to the *VPN Client Administrator's Guide*, Chapter 3, for details on the configuration options.

For the initial release, the update-4.6.00.0045.zip file provided is for use by users who participated in the Beta program so that they may use AutoUpdate to upgrade their Beta clients to the released version. Otherwise, the update file adds no value to users installing the initial version 4.6 Windows VPN Client other than reviewing its contents to become familiar with its components.

Browser Proxy Configuration

Browser proxy configuration is **ONLY** available using the Release 4.1.6 VPN Concentrator code.

During mode config, the VPN Client negotiates a new mode config attribute to determine whether to change the value of a user's browser proxy setting. The VPN Client administrator controls the setting of the attribute through a parameter in the PCF file. This feature is being implemented for Windows (all platforms) only and for Internet Explorer only.

You can configure the VPN Concentrator to push proxy configuration settings into Microsoft Internet Explorer when Windows clients connect to it. The settings are on the **Client Config** tab of Group configuration. You can configure the VPN Concentrator to not modify proxy settings ("Do not modify proxy settings"), to push settings to disable existing proxy configuration ("No Proxy Settings"), to push settings to auto-detect a proxy ("Auto-Detect Proxy settings"), and to push explicit proxy settings ("Use Proxy Server/Port listed below").

With the "Use Proxy Server/Port listed below" setting, you can push a proxy server address, a proxy exception list, and whether the browser will exclude the proxy for local addresses.

After disconnecting, proxy settings are restored to what they were before the VPN connection was established. If a workstation is improperly shut down or rebooted while a VPN connection is established, proxy settings will be restored on boot-up.

VPN Client API Support

Release 4.6.00 provides an API for performing VPN Client operations without using the command-line or GUI interfaces that Cisco provides. To obtain documentation, a sample program, or help for the use of the API please send mail to vpn-client-api-support@cisco.com.

Connect on Open

Connect on open lets a user connect to the default user profile when starting the VPN Client. This feature is implemented on all platforms except Linux and Solaris.

You can configure the Windows and Macintosh VPN clients to connect automatically to the default connection profile when the VPN Client is launched. Configure this in the “Options” dialog of the VPN Client, by checking the “Auto-connect to Default on open” check box.

Section 508 Accessibility Compliance

Release 4.6.x brings the VPN Client in compliance with all Section 508 standards for accessibility. This feature is implemented on all Windows platforms.

Maximum Preshared Key Length is 128 Characters

The maximum pre-shared key length for the VPN Client is now 128 characters. The previous limit was 32 characters. The increased key size works only with central-site devices that support 128 characters (for example, an ASA device). If the central-site device does not support 128 characters (for example, a VPN 3000 Concentrator), you would receive the same log messages as if the pre-shared key were wrong. The log messages are as follows:

```
386 15:39:39.010 03/30/05 Sev=Warning/3IKE/0xE3000056
The received HASH payload cannot be verified
```

```
387 15:39:39.010 03/30/05 Sev=Warning/2IKE/0xE300007D
Hash verification failed... may be configured with invalid group
password.
```



Note

These log messages might change in the future.

Benign Connection Message Removed

When the VPN Client connects to an ASA device using IPSec over TCP, the Client no longer logs the following message:

```
973 10:10:00.619 03/29/05 Sev=Warning/2 IPSEC/0x6370001E Unexpected
TCP control packet received from 10.10.10.10, src port 10000, dst port
1495, flags 18h.
```

This benign but extraneous message has been removed.

Initialization Status Splash Screen Display -- Changed Requirements

Rebranded splash-screen graphics must now be at least 280 pixels wide to accommodate the box that displays the status text. There must be a full-width blank area at the bottom of the graphic at least 36 pixels in height.

New Command Line Argument Allows Minimization on Startup

The command line for the VPN Client now has a new argument that minimizes the VPN Client to the system tray on startup. Administrators can now append **/minimized** to the VPN Client shortcut to achieve this behavior on users' computers.

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 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 4.6 of the VPN Client software.

In addition, you should be aware of the open caveats regarding this release. Refer to “Open Caveats” on page 36 of these Release Notes for the list of known problems.

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.

No Support for ipdptp Dialup Interface on Solaris

VPN Client Releases 3.7.2 and higher no longer support the ipdptp dialup interface on Solaris platforms.

Windows Interoperability Issues

The following known issues might occur with the indicated Microsoft Windows operating systems and applications software.

**Note**

Do not upgrade to Release 4.6.0.3.21 if you depend on Split DNS configurations.

Microsoft Internet Connection Sharing Incompatible

The VPN Client is not compatible with Microsoft ICS (Internet Connection Sharing (ICS) on the same PC.

WINS Support

On Windows 95 and Windows 98, dynamic WINS support works with DHCP-enabled adapters (for example, PPP or NIC adapters that get their IP information dynamically). For static configurations, users must manually configure the adapters with WINS information.

VPN Client Cannot Launch Microsoft Connection Manager

The VPN Client does not see a dialup connection made with Microsoft Connection Manager because of incompatibilities between the requirements of the two applications.

Windows 98 Might Hang on Shutdown

On some Windows 98 PCs with the VPN Client installed, if you restart the PC, it may stop responding (that is, “hang”) on the screen that says “Windows is shutting down”.

Wait a minute. If the PC is still not responding, press the reset button. When the PC reboots, it should not run through ScanDisk, indicating the shutdown was successful in closing all open files. This problem may occur on some PCs and not on others, and we are looking for a solution. Windows 98 shutdown has numerous issues, as can be seen the following Microsoft Knowledge Base Article:

“Q238096 - How to Troubleshoot Windows 98 Second Edition Shutdown Problems”.

Windows 2000 (only) Requires Adding Client for MS Networks for Dialup Connections

For the Cisco VPN Client running on a Windows 2000 system, you cannot access Microsoft resources unless you add the Client for Microsoft Networks for the Dial-up adapter.

Aladdin Runtime Environment (RTE) Issue with Windows 2000

Using versions of the Aladdin Runtime Environment (RTE) on Windows 2000 can cause the following behavior. The login prompt that is posted by the Aladdin etoken when connecting the VPN Client can get hidden in the background. If this happens, the VPN connection can timeout and fail with the following event:

“System Error: Connection Manager failed to respond.”

A side effect of this is that the VPN Client's service and dialer might become out of synch, and the PC might need to be restarted. To avoid this issue, use the Aladdin Runtime Environment (RTE) version 2.65 or later.

Microsoft MSN Installation

Microsoft's MSN installation fails if you have already installed the VPN Client. Uninstall the VPN Client before you install MSN. After MSN has completed installation, you can install the VPN Client.

WINS Information Might Not Be Removed from Windows Servers If Not Disconnected Before Shutdown

If the VPN Concentrator is configured to send WINS server addresses down to the VPN Client and the PC is shut down or restarted without first disconnecting the VPN Client, the WINS servers are not removed from the network properties. This might cause local PC registration and name resolution problems while not connected with VPN.

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

- Be sure to disconnect the VPN Client before shutting down. If you are having problems, check your network properties and remove the WINS entries if they are not correct for your network.
- Alternatively, enable "Disconnect VPN connection when logging off". Go to Options > Windows Logon Properties, check Disconnect VPN connection when logging off.

DNS

For DNS resolution, if the DOMAIN NAME is not configured on the network interface, you need to 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.

Network ICE BlackICE Defender Configuration

Network ICE's BlackICE Defender is a traffic monitoring security product. If you properly configure it, BlackICE Defender can work with the VPN Client. You must configure BlackICE Defender for Trusting, Nervous, or Cautious mode. If you use Nervous or Cautious mode, add the public IP address of the VPN Concentrator to the list of trusted addresses. You can now configure the VPN Client to work with BlackICE Defender configured for Paranoid mode when in Tunnel-everything mode. Split Tunneling requires BlackICE to be in Trusting, Nervous, or Cautious mode.

The Cisco VPN Client firewall has the following requirements for BlackICE (BlackICE Defender 2.5 or greater or BlackICE Agent 2.5 or greater). For BlackICE Defender 2.5, copy the BICTRL.DLL file from the Cisco installation release medium to the BlackICE installation directory on the VPN Client PC. This is a mandatory step for making a connection requiring BlackICE.

BlackICE Defender version 2.9 and greater includes the BICTRL.DLL file in the Network ICE distribution medium, so that you do not need to copy it from the Cisco installation release medium.

Microsoft Outlook Error Occurs on Connection or Disconnect

The following Microsoft Outlook error might occur when the VPN Client connects or disconnects:

“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.”

This message does not affect operation of the VPN Client. The issue occurs when Microsoft Outlook is installed but not configured for email, although it is the default mail client. It is caused by a Registry Key that is set when the user installs Outlook.

To eliminate this message, do one of the following:

- Right-click the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail as the default mail client.
- Use Internet Explorer to configure the system to have no default mail client.
- Configure Outlook as the default mail client.

Adjusting the Maximum Transmission Unit (MTU) Value - Windows Only

VPN Encapsulation adds to the overall message length. To avoid refragmentation of packets, the VPN Client must reduce the MTU settings. The default MTU adjusted value is 1300 for all adapters. If the default adjustments are not sufficient, you may experience problems sending and receiving data. To avoid fragmented packets, you can change the MTU size, usually to a lower value than the default. To change the MTU size, use the VPN Client SetMTU utility. If you are using PPPoE, you may also have to set the MTU in other locations. Refer to the following table for the specific procedures for each type of connection.

The MTU is the largest number of bytes a frame can carry, not counting the frame's header and trailer. A frame is a single unit of transportation on the Data Link Layer. It consists of header data, plus data that was passed down from the Network Layer, plus (sometimes) trailer data. An Ethernet frame has an MTU of 1500 bytes, but the actual size of the frame can be up to 1526 bytes (22-byte header, 4-byte CRC trailer).

Recognizing a Potential MTU Problem

If you can connect with the Cisco VPN Client but cannot send or receive data, this is likely an MTU problem. Common failure indications include the following:

- You can receive data, such as mail, but not send it.
- You can send small messages (about 10 lines), but larger ones time out.
- You cannot send attachments in email.

Setting the MTU Value

If you are *not* experiencing a problem, do *not* change the MTU value. Usually, an MTU value of 1300 works. If it doesn't, the end user must decrease the value until the Cisco VPN Client passes data. Decrement the MaxFrameSize value by 50 or 100 until it works.

The following table shows how to set the MTU value for each type of connection.

Connection Type	Procedure
Physical Adapters	Use the SetMTU utility supplied with the Cisco VPN Client.
Dial-up	Use the SetMTU utility supplied with the Cisco VPN Client.
PPPoE - All Vendors	<p>Windows XP only</p> <p>Use SetMTU</p>
PPPoE - EnterNet	<p>Windows 98</p> <ul style="list-style-type: none"> • On the main desktop, right click on My Network Places and go to Properties. The Network window opens. • Double-click the Network TeleSystems PPPoE Adapter. • On the Network TeleSystems window, click the Advanced tab, and then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400. <hr/> <p>Windows 2000</p> <ul style="list-style-type: none"> • On the main desktop, right-click My Network Places and go to Properties. The Network and Dial-Up Connections window opens. • Right-click and go to Properties on each connection until you find the connection that has the NTS EnterNet PPPoE Adapter. • Once you find the correct connection, click Configure on the right side of the window. • On the next window, click the Advanced tab, then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

Connection Type	Procedure
PPPoE - WinPoet	<p>Windows 98: WinPoet does not provide user control over the PPPoE MTU under Windows 98.</p> <p>Windows 2000</p> <p>WinPoet does not provide a user interface to control the MTU size, but you can control it by explicitly setting the following registry key:</p> <p>HKLM/system/currentcontrolset/control/class/<guid>/<adapternumber> adapter(000x): Value: MaxFrameSize Value type: DWORD Data: 1300 (or less)</p> <p>The GUID and adapter number can vary on different systems. Browse through the registry, looking for the MaxFrameSize value.</p> <p> Caution Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable.</p>
PPPoE - RasPPPoE	<p>Windows 98</p> <ul style="list-style-type: none"> • On the main desktop, right-click My Network Places and go to Properties. The Network window opens. • Find the PPP over Ethernet Protocol that is bound to the Network card that is in your PC, then double click on it. • In the General Tab check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400. <p>Windows 2000</p> <ul style="list-style-type: none"> • On the main desktop, right-click My Network Places and go to properties. The Network and Dial-Up Connections window opens. • Right-click the connection the PPPoE Protocol was installed to, and go to properties. • When the window opens, double-click PPP over Ethernet Protocol. • In the General Tab, check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.

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/routers/index.html>
- 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.

VPN Dialer Application Can Load During OS Shutdown or Restart

When using the VPN Client's Start Before Logon feature in "fallback" mode on Windows 2000 or XP, the VPN dialer application loads during a shutdown or restart of the operating system. This will not cause any problems and can be ignored.

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.

AOL 7 Disconnects after VPN Authentication

When making a dialup connection with AOL 7.0 Revision 4114.537 (for Windows 95, 98, ME, Windows 2000 and XP), then attempting to connect with the VPN Client, AOL might disconnect while the user is being authenticated. This is an AOL issue, not a VPN Client problem.

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.

The workaround is to try to reconnect the dialup connection to 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.

Issues Loading Digital Certificate from Microsoft Certificate Store with IE 4.0 SP2

The following error occurs in the VPN Client log when using a Digital Certificate from the Microsoft Certificate Store. This can occur with Internet Explorer 4.0 with SP2 and using the VPN Client v3.1 or v3.5:

```
“Could not load certificate cn=Joe  
Smith,ou=Engineering,o=MyCompany,l=Buffalo, st=new  
york,c=US,e=jsmith@mycompany.com from the Unsupported Store store”
```

Both the VPN Client and the Certificate Manager can see and validate the Certificate, but when you try to connect using that Certificate, you get a message in the Connection History dialog that says, “Failed to establish a secure connection to the security gateway”.

To fix this problem, do *one* of the following:

- Upgrade to Internet Explorer v5.0 or greater.
- Upgrade the PC to Service Pack 6.0a.

Requirements for using VPN Client for Windows Using Digital Certificate With Non-exportable Keys

To use certificates with non-exportable keys, you must have the VPN Client, Release 3.6, 4.0 or 4.6, and your PC must have Internet Explorer version 5.0 SP2 or later installed to function properly.

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 System Tray Icon Might Erroneously Indicate Logout

When using VPN Client with Start Before Logon (Windows 2000) and Entrust Entelligence, the Entrust system tray icon indicates that it is “logged out” once in Windows. It is really logged in, just not in the normal Windows desktop. The reason for this is that the context that Entrust was logged into was on the “Logon desktop”. This is an Entrust issue, not a VPN Client problem.

Entrust operates normally once logged into within Windows.

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.

Use Entrust Entelligence 4.0 with VPN Client Release 3.5.1 or 3.1 Start Before Logon

When using the Release 3.5.1 or 3.1 VPN Client with the Entrust Entelligence 4.0 software, the Start Before Logon feature does not function properly. Upgrading to Entrust Entelligence 5.1 resolves this problem.

Some Entrust Dialogs Do Not Display Properly When Using VPN Client Start Before Logon

When using the VPN Client with Start Before Logon and Entrust Entelligence, some Entrust dialogs do not display properly on the logon desktop that displays before going into Windows 2000. The first time the VPN Client dialer and service access the Entrust certificates, it prompts for a security check. This prompt displays in Windows, but not at the logon screen.

To work around this problem, connect the VPN Client once, while in Windows and after installing, to register the VPN applications (ipsecdialer.exe and cvpnd.exe) with Entrust. Once you have done this you can use it at the logon desktop.

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.

ZoneAlarm Plus Versions 3.1.274 and Earlier Are Incompatible with VPN Client

The following known incompatibility exists between the Cisco VPN Client and Zone Labs ZoneAlarm Plus version 3.1.274 and earlier. If you are using such a version of ZoneAlarm Plus, please visit <http://www.zonelabs.com> or contact your Zone Labs representative for an update.

On a PC with ZoneAlarm Plus version 3.1.274 (or earlier) and the VPN Client, the following errors occur when the PC boots:

On Windows 2000:

ZAPLUS.exe has generated errors and will be closed by Windows. You will need to restart the program.

An error log is being generated.

The Application Log states:

The application, ZAPLUS.EXE, generated an application error. The error occurred on 7/23/2002... The exception was c0000005 at address 00401881 (<nosymbols>).

Similar errors occur on other Windows operating systems.

The result of this error is that the ZoneAlarm GUI does not run, and therefore a user can not change any settings in ZoneAlarm Plus or allow new programs to access the Internet.

ZoneLabs Automatically Adds Loopback and VPN 3000 Concentrator Addresses to Trusted Zone for Windows NT PCs

The Loopback address and the VPN 3000 Concentrator's address are automatically added to the ZoneLabs “Trusted Zone” on Windows NT-based systems.

If a Windows NT based-PC has ZoneAlarm, ZoneAlarm Pro, or Zone Labs Integrity Agent, and the VPN Client Release 4.0 installed on it, the loopback address (127.0.0.1) is automatically added to Zone Labs “Trusted Zone” when the Client service is started. Additionally, the VPN 3000 Concentrator’s address is automatically added to the “Trusted Zone” when a connection is made.

Upgrading Zone-Alarm Pro to Version 3.7.098 Causes Error When VPN Client Is Already Installed on the PC

Upgrading ZoneAlarm Pro version 3.5.xxx to ZoneAlarm Pro version 3.7.098 when the VPN Client is installed on the PC might cause the following error to appear:

“The procedure entry point DbgProcessReset could not be located in the dynamic link library VSUTIL.dll.”

Click OK, and the installation continues. See ZoneLabs bug number 10182.

Harmless Warning Might Occur with Linux Kernel 2.4

Linux users running 2.4 kernels may encounter the following warning when the VPN Client kernel module is loaded:

Warning: loading /lib/modules/2.4.18-3/CiscoVPN/cisco_ipsec will taint the kernel: no license

This message indicates that the VPN Client kernel module is not licensed under the GPL, so the Linux kernel developers will not debug any kernel problems that occur while this kernel module is loaded. This message does not affect the operation of the VPN Client in any way.

DHCP Route Renewal in Windows 2000 and Windows XP

In a Windows 2000 or Windows XP environment, if the public network matches the private network (for example, a public IP address of 192.168.1.5, with a subnet mask of 255.255.0.0, and an identical private IP address) and the public

network's route metric is 1, then traffic might not be tunneled to the private network. The same problem can occur if you are using a virtual adapter and the public metric is smaller than the virtual adapter metric.

In Windows 2000 and Windows XP, you can increase the metric of the public network by doing the following steps:

-
- Step 1** Select Start > Settings > Control Panel > Network and Dial-up Connections.
 - Step 2** Select the public interface and click properties for the public interface.
 - Step 3** Select Internet Protocol (TCP/IP) and get the properties for the Internet Protocol (TCP/IP).
 - Step 4** Click Advanced, and set the interface metric to 2 or greater.
-

Solaris Client Using Routed RIP Might Lose Connectivity

If the VPN Client running in the Solaris environment uses routed RIP to learn its default route, you might lose connectivity. This is because RIP is blocked when the VPN Client is connected in all tunneling mode.

Data Meant for Private Network Stays Local if VPN Client's Local Network Is on Same IP Subnet as Remote Private Network

This problem occurs only with the VPN Client, Release 4.6 and only with Virtual Adapter (Windows 2000 and Windows XP), when the VPN Client's local network is on the same IP subnet as the remote private network. When a VPN connection is up, data meant for the private network stays local. For example: 192.168.1.0/255.255.255.0

The VPN Client, Release 4.6, with Virtual Adapter attempts to modify local route metrics to allow data to pass over the VPN tunnel. In some cases, it is impossible for the VPN Client to make this modification.

To work around this problem, make the change manually, using the following procedure:

-
- Step 1** Run > Control Panel > Network and Dialup Connections.
 - Step 2** Right-click on the adapter in question and select Properties.
 - Step 3** From the Adapter Properties dialog, select TCP/IP from the list and click Properties.
 - Step 4** Click Advanced and increase the number in the “Interface metric” box by 1 (it is usually 1, so making it 2 works).
 - Step 5** Click OK to exit out of all dialogs.
 - Step 6** The VPN connection should now work.
-

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 is 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.

VPN Client Supports Sygate Personal Firewall V. 5.0, Build 1175

The supported version of Sygate Personal Firewall is version 5.0, build 1175. Earlier versions might cause the following Blue screen to occur on a Windows NT-based system that has made many connects/disconnects with the VPN Client:

Stop: 000000d1 (BAD0B0B8, 00000002, 00000000, BFF12392)

Driver_IRQL_Not_Less_Or_Equal

***Address BFF12392 base at BFF10000, Datestamp 3CCDEC2C - Teefer.sys

The 4.6 VPN Client Is Not Supported on Windows 95

The VPN Client for Windows, Release 4.0 and higher, requires the use of the Windows 98 or later operating system. We recommend updating your operating system to a newer version of Windows.

VPN Client Not Supported on Windows NT Servers

The VPN Client is not supported on any Windows NT server version (including Windows 2000 and Windows XP/.NET/2003 servers).

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 directory and are date and time stamped. There is no limit to the size of the log when logging is enabled. The file will continue 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.

Start Before Logon and Microsoft Certificate with Private Key Protect Fails

Trying to connect the VPN client using Start Before Logon (SBL) and Microsoft Machine-based certificates fails. This is a Microsoft issue, not a VPN Client problem.

If your certificate has private key protection enabled, every time you use the certificate keys you are either prompted for a password to access the key, or notified with a dialog and asked to click OK.

The prompt displayed when using a certificate with private key protection appears on the Windows Desktop. You do not see this message while at the “Logon” desktop, therefore the VPN Client cannot gain the access to the certificate needed to connect.

Use *one* of the following workarounds:

- Get a certificate without private key protection (just make sure it is machine-based, otherwise it won't be accessible before logging on).
- Instead of using Start Before Logon, log on to the PC using cached credentials, make the VPN connection, and— using the “stay connected at logoff” feature—logoff/logon with the VPN established to complete the domain logon.

Downgrading VPN Client from Release 4.6 Causes Start Before Logon Failure

Start Before Logon fails if the VPN Client is downgraded from Release 4.6 to 3.6. The reason for this is that the file `csgina.dll` is upgraded when the VPN Client version 4.6 is installed. If the VPN Client is downgraded to version 3.6, the `csgina.dll` file for version 4.6 is not replaced, and this breaks ability in the VPN Client version 3.6 to Start Before Logon.

Follow this procedure to drop back to the VPN Client version 3.6 from version 4.6.

-
- Step 1** Uninstall the VPN Client version 4.6.
 - Step 2** After rebooting, search for `csgina.dll`. This file is found in the System32 directory.
 - Step 3** Rename `csgina.dll` to something like `csgina.old`.
 - Step 4** Install the VPN Client version 3.6.
-

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 Can Require Smart Card When Using Certificates

For Windows 2000 and Windows XP systems, you can configure the VPN Client to require the presence of a Smart Card when Certificates are used. If this feature is configured, the VPN Client displays an error message if a Smart Card is not present. The Certificates need not be present on the Smart Card itself. To configure this feature, add the following line to the user's client profile, specifying the appropriate vendor for your Smart Card:

```
SmartCardName=<Name of Smart Card Vendor>
```

If you are using pre-shared keys instead of Certificates, this requirement is not enforced, even if configured.

To disable the Smart Card verification function, completely delete the entry: SmartCardName=<text> from the user's client profile.

Mutual Group Authentication Requires a CA Certificate

A CA certificate must be configured on VPN client if you use a profile for mutual group authentication (IPSec Hybrid mode).

The VPN client can access the Microsoft stores where CA certificates may already be available. However, VPN Client enforces the configuration of one CA certificate. It produces an error if it fails to do so.

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.

Use Zone Labs Integrity Server 2.1.052.0 or Higher with VPN Client 4.0

Versions of the Zone Labs Integrity Server earlier than 2.1.052.0 exhibit the following problem. If two or more VPN Clients (running on Windows 2000 or XP) are connected to a VPN 3000 Series Concentrator and receive firewall policy from a ZoneLabs Integrity Server, the Integrity Server registers only one connection.

On the Integrity Flex (client agent), under “Policies”, the “Integrity Server” column flashes “Connected” then “Disconnected” over and over. Also, the VPN Client log includes the following event: “The firewall, configured for Client/Server, returned a status of lost connection to server.” Zone Labs Integrity Server version 2.1.052.0 fixes this issue.

Restart VPN Client Service If You Install VPN Client Before Zone Alarm

The Firewall Enhancement, “Prevent VPN Traffic Blocking”, automatically adds the Loopback address (127.0.0.1) and the address of the VPN 3000 Concentrator to the ZoneAlarm or ZoneAlarmPro trusted zone.

An exception to this, however, occurs if the VPN Client is installed before Zone Alarm. Then the VPN Client’s service must be restarted by rebooting the PC or stopping and restarting the service through the Control Panel (on Windows NT-based PCs).

InstallShield Error Might occur during VPN Client Installation

The following error message might occur during VPN Client installation:

IKernel.exe - Application Error

The instruction at “0x771c741a” referenced memory at “0x00163648”. The memory could not be “read”.

This error is caused by an InstallShield component, possibly because of a run-once stale remnant. To recover, you must reboot.

The InstallShield Knowledge base article q108020 addresses this problem. To view this article go to the following URL:

<http://support.installshield.com/kb/view.asp?articleid=q108020>

Microsoft has a fix for this issue. For more information and to obtain the fix, go to the following URL:

<http://support.microsoft.com/default.aspx?scid=kb;en-us;329623>

VPN Client cTCP Connection Fails If Checkpoint Client Is Installed

When the Checkpoint VPN-1 Securemote client is installed with the 4.6 VPN Client, and the VPN Client attempts to connect using cTCP, the 4.6 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 Securemote is installed, you must disable the Check Point SecuRemote driver in the Connections Properties. To do this, you must be administrator. Follow these steps:

-
- Step 1** Click Start > Settings > Control Panel > Network and Dial-up Connections.
 - Step 2** Select the Local Area Connection you use.
 - Step 3** Click on File > Properties.
 - Step 4** Uncheck Check Point SecuRemote, and click OK.
-

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.

- 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 every time this question appears. 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 (etabcgina.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” token: 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” token 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 Windows XP; we have not checked Windows 98.

- 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 4.0VPN 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 Internet 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.

- CSCdy68888

On a Windows 98 PC that has the Sygate Personal Firewall, the following message may appear in the VPN Client log file:

“Packet size greater than ip header”

This message does not interfere with the VPN Client’s ability to pass data and can be ignored.

- 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.

- CSCdy79358

The following error might occur on Windows 98 when making many VPN connections without closing the VPN Client between connections:

VPNGUI caused an invalid page fault in module MSVCRT.DLL at 0167:78002f52.

To avoid this error, exit the VPN Client after disconnecting.

- 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 | 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.
-

- 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.

- CSCea56044

Cisco VPN Client cannot differentiate two digital certificates with same CN. If two digital certificates have the same CN (complete DN might be different), VPN Client software cannot use the second one; it always takes the first certificate matching this CN.

Workaround:

Use a different CN.

- 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.

- CSCed26068

Using VPN Client, Release 4.0.3.C running under Windows 95, Windows 98, or Windows ME, we can not log in to the Microsoft network using the Command-Line Interface to connect VPN communication. NetBIOS packets fail to be encrypted.

- CSCee08782

Mac OS X VPN Client Release 4.0.3.E and higher 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.

- 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.

- CSCeg59048

The Linux VPN Client with Virtual Adapter fails to function properly when using subinterfaces.

Workaround:

Do not use subinterfaces in conjunction with the Linux Virtual Adapter VPN Client. Make connections routed only through the main interface, such as eth0, *not* eth0:1.

- CSCeh15956

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

- 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.

- CSCeh54674

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

- CSCei03756

While using the Linux 64-bit capable client, the following error appears when a connection attempt occurs:

The application was unable to communicate with the VPN sub-system.

This usually appears when a VPN Client has been disconnected and reconnected quickly, without enough time for the Client to properly shut down.

Workaround:

Use the following commands in this order:

```
killall -9 cvpnd  
vpnclient disconnect
```

The VPN Client should now be ready to reconnect.

- 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.

- 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/smartcard.

The following message appears in the VPN Client logs:

```
"IKMPLogin' 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 can't access some private networks; that is, networks behind the VPN 3000 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.

Resolved Caveats

The following sections list the caveats resolved in each release. For your convenience, releases that are not platform-specific are listed first. All other resolved caveats are listed by operating system, with the most recent release first. Within each grouping, resolved caveats are listed in ascending alphanumeric order.

- [Caveats Resolved in All VPN Clients, page 61](#)
- [Caveats Resolved in VPN Clients for Windows,, page 64](#)
- [Caveats Resolved in VPN Clients for Linux, page 75](#)
- [Caveats Resolved in VPN Clients for Solaris, page 78](#)
- [Caveats Resolved in VPN Clients for Mac OS X, page 79](#)

Caveats Resolved in All VPN Clients

The following resolved caveats are not operating-system-specific.

- [Caveats Resolved in Release 4.6.04, page 61](#)
- [Caveats Resolved in Release 4.6.03, page 61](#)
- [Caveats Resolved in Release 4.6.02, page 62](#)
- [Caveats Resolved in Release 4.6.01, page 63](#)

Caveats Resolved in Release 4.6.04

- CSCei26444
VPN Service does not start after installing 4.6.04.0043 VPN Client on Windows 98 SE. Installing the 4.6.04.0043 client on Windows 9x, all other Windows operating systems are not effected.

Caveats Resolved in Release 4.6.03

- CSCea93535
Performance issues exist with H.323 and the 4.0 VPN Client virtual adapter. These performance issues could be related to MTU.
- CSCeb42449
On a Windows XP PC with the 4.0 or 4.0.1 VPN Client a user might experience DNS issues upon connection. After connecting to a (4.0) VPN 3000 Concentrator, the Client can ping resources on the private network by IP, but not by name. Once this happens on the Windows XP system, you can go to network connections->advanced->advanced settings and change the order of the adapters, or actually move a different one (does not matter which) to the top of the list and hit OK. You can then ping by name.

If you disconnect the VPN Client and reconnect, you get the same results, but the adapter at the top of the list is the one you moved there previously. However, you cannot ping by name until you move a different adapter to the top of the list and hit OK.

This is not reproducible with a Release 3.6.x VPN Client on Windows XP or on Windows 2000 with any client tested (Tested only Windows XP and 4.0/4.0.1 VPN Clients).

This is a known Microsoft issue. Please refer to:

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q286/8/34.asp&NoWebContent=1>.

A feature request has been submitted to change the registry key for this.

- CSCeb67454

With the VPN Client, Release 4.x on Windows XP, using split tunneling and split DNS, the DNS lookup does not use the right DNS servers.

If you encounter this bug, the following things need to be true:

1. All or nothing tunnel works fine.
2. This problem occurs only with split tunnel and split tunnel with split DNS
3. If you use nslookup to resolve the ping'd server, it might give the right info.
4. This problem exists for both FQDN and unqualified name.



Note See also the resolved caveat CSCeb42449, of which this is a duplicate.

- CSCeg78409

This is a documentation bug. The “ForcedKeepalives” profile parameter is not documented in vpnclient 4.0 and 4.6 administrator guide. It was properly documented in 3.6 documentation:

- CSCeh40276

Using VPN Client on Virtual Adapter platform, some routes might be incorrectly pointing to the virtual adapter interface.

Caveats Resolved in Release 4.6.02

- CSCdz23397

Certificates exported from Netscape 7 do not import into the VPN Client. All of the current VPN Clients exhibit this symptom with this version of Netscape. Previous versions of Netscape are still compatible with the VPN Clients.



Note This caveat, which has now been resolved, was previously included under “Usage Notes” in earlier Release Notes.

- CSCee60154

After making a VPN Client connection, some traffic types no longer work. Specifically applications that send large packets like SMTP, HTTP, and SSH.

The 2.6.4 Kernel enabled a feature of certain Ethernet cards that discards packets larger than the configured MTU. Since the VPN Client lowers the MTU visible to the applications in order to add its overhead without exceeding the original MTU, the resulting packets are bigger than the newly configured MTU. Therefore the card throws out the large encrypted packets.

Caveats Resolved in Release 4.6.01

- CSCea44601

The VPN Client does not put any limit to the number of log files that are saved in the \VPN Client\Logs directory. Users must manually delete these files to remove all or some of them.

- CSCsa41980

In rare cases in which IKE packets are fragmented and received out of order, it is possible for the Cisco VPN Client to terminate abruptly.

Errors about invalid header appear, such as:

```
ISAKMP header invalid: Invalid version 11.1 found
```

The error message:

```
cvpnd.exe has generated errors and will be shut down
```

also occurs. Symptoms are more likely in cases (such as certificates) in which large IKE packets are produced. The packets need to be received at the client end out of order (such as load-balancing).

This issue is not observed if packet does not use transparency (UDP, TCP, or NAT-T).

Caveats Resolved in VPN Clients for Windows,

The following sections list the resolved caveats for each release of the 4.6.x.y Windows VPN Client.

- [Caveats Resolved in VPN Client for Windows, Release 4.6.04.0043, page 64](#)
- [Caveats Resolved in VPN Client for Windows, Release 4.6.03.0021, page 65](#)
- [Caveats Resolved in VPN Client for Windows, Release 4.6.2.0011, page 69](#)
- [Caveats Resolved in VPN Client for Windows, Release 4.6.01.0019, page 71](#)
- [Caveats Resolved in VPN Client for Windows, Release 4.6.00.0045, page 74](#)

Caveats Resolved in VPN Client for Windows, Release 4.6.04.0043

- CSCeh24116
While using AutoInitiation, the banner appears multiple times if left unattended. With a banner enabled, every time the VPN Client disconnects and reconnects, the banner appears with each successful connection.
- CSCeh14815
If dashes are in path, MSI does not copy pcf and ini files. The customized vpnclient.ini and .pcf files are not copied to targeted folder (C:\Program Files\Cisco Systems\VPN Client) even if MSI installation is finished and then PC is rebooted. This symptom occurs only on MSI when the folder name to specify in the WinZip Self-Extractor box includes “-” (for example, vpn-client).
- CSCeh62339
Split DNS no longer works properly with the Windows VPN Client, version 4.6.03.0021. A side effect of another fix prevents Split DNS from working properly. The feature now tunnels all DNS through the tunnel, instead of tunneling only the pushed split domain list.
- CSCsa70552
The VPN Client cancel connect does not work with MS automatic ip disabled. A PC gets a DHCP IP address from network A. The same user moves to Network B. If DHCP fails, with MS automatic IP disabled, the PC gets the last assigned ip, which is that of network A. This is an invalid IP address for network B. Now, when the user tries to connect using the VPN Client, the log

window constantly displays the following message: 6 15:42:05.026 02/24/05 Sev=Warning/2 CVPND/0xA3400018 Output size mismatch. Actual: 0, Expected: 237. (DRVIFACE:1341)

The “cancel connect” does not work, and this messages displays forever.

- CSCsa72910

If you initiate a VPN connection with the VPN Client when there is no physical network connection, the VPN Client tries about 600 times in about 2 minutes before it times out with the following message: “610 15:38:23.007 02/24/05 Sev=Info/4 IKE/0x63000075 Unable to acquire local IP address after 600 attempts (over 600 seconds), probably due to network socket failure.”

During this time the “cancel connect” does not work.

- CSCsa76773

The Cisco VPN Client Virtual Adapter (VA) always reports its speed as 1 Gbps. Some user level applications base things to do on the connection speed. For example, if an end-user using dialup and Outlook brings up a VPN connection, we would claim our speed to be 1 Gbps. Outlook then thinks it has a lot of bandwidth and decides to download the whole mail messages instead of just headers.

- CSCsa78460

If the VPN Client pcf file is imported and the associated certificate does not exist, then upon connection, the VPN Client fails. The previous version of the VPN Client showed an error message indicating that the associated certificate does not exist, and that version does not fail.

- CSCsa90252

VPN GUI may not appear if a user logs into the computer too quickly while using Start Before Logon (which results in user logging using cached credentials).

Caveats Resolved in VPN Client for Windows, Release 4.6.03.0021

- CSCeb04745

Can't Install the Virtual Adapter, This happens because some of the VPN 5000 Registry keys are not removed by the Uninstall.

- CSCed84982
No lock icon appears in the VPN Client GUI when the connection entry name has a leading space. This appears to be a cosmetic issue. The VPN connection is established. The lock icon does appear in the systray.
- CSCee13237
When multiple users log in to Windows XP, the VPN username/password prompt window always shows up in the first user's desktop. No other users can see this window when opening a VPN connection. They may think the VPN client is stuck. This conditions happens when fast user switch mode is selected and user doesn't login first.
- CSCeg05250
If incorrect username/password credentials are used with the 4.6.00.0045 VPN Client command line, they are saved and used without prompting for new user/password. This also affects the GUI, in that the bad credentials are saved in the .pcf file and are used when you try to connect with the same profile through the GUI.
- CSCeg34848
When using auto-initiation of the VPN Client and initiating it for all types of network traffic, when you boot the PC, the VPN Client tries to connect to the central site *before* the VPN service has started. This results in an error message appearing every time the PC boots up:
Error 201: VPN Subsystem not available
Clicking OK on this error window lets the auto-initiation proceed, and the client does connect correctly, but the error is a bit disconcerting for users. Need to either delay auto-initiation until the VPN service has had a chance to start properly, or at least prevent the error message from appearing.
- CSCeh13171
VPN Client crashes when using Radius password expiry feature. Manipulating the domain field causes the Client to fail.
- CSCeh13176
Using Radius with password expiry, a saved password may never be cleared using the VPN Client GUI. Conditions The password should be able to be erased, but the GUI does not allow it.

- CSCeh19087
Autoupdate and Client Update Notifications fail if Force Network Login is in use. Force net login preempts these notifications until the GUI is relaunched.
- CSCeh37605
A fatal exception error occurs after KB891711 is applied on Windows 98. Microsoft has addressed this issue with a new version of this update on their update download page.
- CSCeh47222
Another ClientLanguage parameter is created after MSI installation with customized vpnclient.ini is launched. For example:

```
[MAIN]
!ClientLanguage=jp
ClientLanguage=
```

This issue occurs only when MSI installation with 4.x is launched. It does not occur when MSI with 3.x or InstallShield (both 3.x and 4.x) is launched.

Workaround:

Use InstallShield

- CSCsa57162
Name resolution takes a long time when going through the tunnel in tunnel everything mode with the client on a Windows XP machine. When connected via tunnel, DNS requests use the ISP assigned DNS server first, and after they time out (since ISP assigned DNS cannot be reached via the tunnel), they use the tunnel-pushed DNS server, causing a delay name resolution.
- CSCsa57346
Cisco VPN Client, Release 4.6.01.0019, installed on a Windows XP system with SP2, when tested by Device Path Exerciser (part of MS HCT v12.0), produces the following error, and fails the test.

```
780.784 : Starting assertion 22.3.1
780.784 : Assertion Title: The driver under test must not blue
screen the system while running driver verifier.
780.784 : Description: Running tests under driver verifier
780.7D0 : +VAR+SEV2      0 : There is a problem with Cisco Systems
VPN Adapter
780.7D0 : +VAR+SEV2      1 : Status code: 0x1802401, Problem code:
0x16
```

```
780.7D0 : +VAR+SEV2      2 : Status codes returned that are
incompatible with testing: DN_HAS_PROBLEM
780.7D0 : +VAR+SEV2      3 : Problem code: CM_PROB_DISABLED
```

- CSCsa57833

A PC running Windows XP, SP 1 and SP@, with both the VPN Client and Virus Buster 2005 (Trend Micro) installed failed when the user tried to activate the VPN Client, Release 4.6.00.45.

- CSCsa59384

VPN Client, Release 4.6.01.0019, does not work right with Microsoft local machine certificate. Errors are as follows:

```
8      11:57:48.554 01/21/05 Sev=Info/4CERT/0x63600014
Could not load private key for certificate cn=<deleted> from store
Microsoft Local
Machine Certificate.
```

```
9      11:57:48.554 01/21/05 Sev=Warning/2IKE/0xE3000007
Unable to open certificate (cn=<deleted>).
If you are using a smartcard or token containing a certificate,
verify the correct one is plugged in and try again.
```

- CSCsa60175

Force Network Login works only when a banner is configured. When a banner is configured, the banner text, the separator, and the warning all display. If no banner is configured, then the warning is not displayed and the user is not logged out.

- CSCsa62440

The MSI version of the 4.6 installer can have an MTU issue. Under default conditions, the VPN Client might drop packets of certain sizes, because we are setting the Virtual Adapter MTU (layer 2) to 1300. This has a problem on the receive-side.

Sometimes, some drivers above the Virtual Adapter (VA) allocate only 1300 bytes of buffer (same as MTU) to copy the packet. But, if the packet received is larger than 1300 bytes, then the packet gets discarded because the drivers above the VA don't have a sufficiently large buffer allocated to copy the entire packet. The fix for this problem is to set the MTU to 1500 at layer2, and 1300 at layer 3.

Caveats Resolved in VPN Client for Windows, Release 4.6.2.0011

- CSCdx57197
If IOS sends a split tunnel attribute that is host-based (255.255.255.255 mask), the VPN Client uses the host in a QM, but it passes the IPV4_ADDR_SUBNET in the ID payload. IOS expects IPV4_ADDR, as this is a host ID. This causes connectivity issues.
- CSCeb22862
Customer is not seeing the xauth prompt from the VPN 3000 Concentrator onto the client machine when logged into Windows XP (home/PRO) system. When there are multiple users are logged in using the FAST SWITCH USER utility on the Windows XP machine, the xauth prompt is always displayed on the first/initial logged-in user while the client was launched by the second user. This showed the same symptoms with the different versions of the VPN client code. I tried on Windows XP PRO and customer has tried on Windows Home edition
- CSCef45028
If Sygate Personal Firewall 5.5 is installed, Windows XP might fail with a blue screen just after the Cisco VPN Client completes IKE negotiations. It doesn't matter whether Sygate is actually on. This problem was observed with Windows XP with SP1 or SP2, using certificate-based or pre-shared key authentication with Cisco VPN 3000, and has been seen with VPN Client releases 4.0.2, 4.0.4 and 4.0.5
- CSCeg04264
Release 4.6 VPN Client error messages are different from those in the Release 4.0.x VPN Clients. With the 4.0.X version of the VPN Client, if there is a problem with the broadband provider, users get the following pop-up: "Secure VPN connection terminated locally by the client. Reason 412: The remote peer is no longer responding."

With the Release 4.6 VPN Client, there is no event message at all, the Client just states that it is not connected. If I enable connect history display, I get the following message: "Secure VPN connection terminated locally by the client. Reason 401: An unrecognized error occurred while establishing the VPN connection. Not connected."

- CSCeg77052

The Windows version of the VPN Client cannot delete only a root certificate. The following is the sequence that caused the error:

1. A root certificate is imported to VPN Client.
2. The VPN Client tries to delete a root certificate.
3. The following error appears, and a root certificate cannot be deleted:

```
-----
Error 33: Unable to delete certificate "xx" from certificate
store.
-----
```

This issue occurs only between 4.0.5(A) and 4.0.5(C)

- CSCeh17709

When using the ForceNetLogin feature the icon tray does not have a VPN icon. This happens with all ForceNetLogin connections.

- CSCeh43162

Start Before Logon now works with Force Net Logon so the following note in the VPN Client Administrators guide on page 2-11 needs to be modified:

Note You cannot use this feature with Start Before Logon. If users are connecting via dialup (RAS), you should add...

Should now read:

Note If users are connecting via dialup (RAS), you should add...

- CSCsa52383

VPN Clients using certificates can successfully connect, authenticate, and pass traffic. But upon reconnecting, Clients receive errors. They are unable to connect until the VPN Client is shut down and restarted. A pop-up error displays message similar to the following: "Unable to connect Reason 437: Bad Parameter". Client logs have an entry similar to the following:

"1 10:45:19.684 01/07/05 Sev=Warning/2 IKE/0xE3000007 Unable to open certificate ([certificate information here]). If you are using a smartcard or token containing a certificate, verify the correct one is plugged in and try again." This problem is observed only in Release 4.6 VPN Client code, and only when using certificates and reconnecting.

- CSCsa46003
Users can't sniff for packets when VPN Tunnel is established. This can happen in multiple ways, but we saw this behavior on:
 - Windows 2000. Windows XP was fine
 - Problem only with inbound packets
 - VPN Client version needs to be 4.0 or higher
- CSCsa52378
On Windows XP PCs, if the VPN Client 4.6.01.0018 is installed and the interface metric is set to the default of auto, the VPN Client does not pass traffic. If the interface metric is changed to anything other than auto, there is no problem.

Caveats Resolved in VPN Client for Windows, Release 4.6.01.0019

- CSCdz58488
The Cisco proprietary NAT Transparency can be enabled in environments where NAT/PAT is not used, but perhaps a firewall allows UDP but not ESP packets. The standards-based implementation does not allow for this option since it is autodetecting the need for NAT transparency based on whether the VPN Client is in a NAT/PAT environment.

The user requested a mechanism per profile to force the use of NAT-T even if client/concentrator does not detect that they are behind a NAT/PAT device.
- CSCeb11271
When trying to import a certificate, on the GUI, the “Unable to import certificate” message is displayed. A password has been provided when generating the Certificate request file. This password has been correctly re-entered in the “Import Password” field.
- CSCeb15093
When a connection is made with the VPN Client using a Certificate that does not contain a password, a command line option 'nocertpwd' was added in order to not prompt the user to enter a password (which there is none) to unlock this certificate. There is no PCF equivalent for this option for a connection not made using the command line. This problem happens only if the certificate is in Cisco store.

- CSCee93255
VPN Client fails when invalid ZL Integrity failover server is set.
- CSCef46893
The VPN Client for Windows using SUB CAs from DOD PKI fails IKE authentication with router with certs from another SUB CA.
- CSCed49306
If a user is member of at least 500 groups in the domain (Win2000), The VPN Client cannot open a connection. The message in the log says that the certificate could not be retrieved because the store is empty. The same user can connect without a problem if the number of groups he or she belongs to is less than 500. The problem was first observed with VPN Client version 3.6.1, and version 4.0.3c also had the problem.
- CSCef50703
Loading a CA certificate that has an incorrect value set for the number of free bits in the cRLDistributionPoints extension will result in the VPN Client's inability to complete the certificate chain.

Certificate xyzCA.cer has only 7 bits turned on (0xFE) in the reasons value of the cRLDistributionPoints extension, but since the unused bit's value is 0, the length of the bit string is 8 bits. If the certificate is intended to follow RFC 2459, then it should use only 7 bits and have the unused bits value set to 1 (0x01 0xFE); then Cert-C 2.0 would be able to read it. If it is intended to follow RFC 3280, then it should use 9 bits and have the unused bits value set to 7 (0x07 0xFE 0x00). However, Cert-C 2.7 (with an additional bug fix) can read the certificate as-is.
- CSCef82642
VPN Client software is unable to verify some user certificates. There is nothing special about these certificates.
- CSCef84479
The VPN Client fails when Sygate firewall is installed and the system is not configured with correct DNS servers.

If the Ethernet/wireless is connected after logging into Windows, and the DNS server is not reachable, then you get warning 201 on the GUI, then you get the XAuth prompt. You are eventually connected, but after the connection, you can't pass any traffic. From the second connection onward, everything works just fine.

- CSCef89651
TunnelEstablished Registry key might be set to 1 if xauth is canceled during a VPN Client connection attempt. The correct setting should be 0.
- CSCef89853
There is currently no way to differentiate certs that have the same common name and reside in the same store. The VPN GUI does not allow users to associate a different cert with same name in the profile.
- CSCef93731
The VPN Client does not append the parent suffix even if the “AppendOriginalSuffix” (under [DNS] section) value is present in vpnclient.ini. A DEBUG log message shows that the correct value was present in vpnclient.ini. Windows network connection property pages also had the right checkbox selected to append the parent suffix.
- CSCsa42416
If Netopia's NetOctopus is installed on the host, the Cisco VPN Client cannot disable the Virtual Adapter at tunnel disconnect.
- CSCsa44461
If there is no character in backup server list (that is, the list is empty), the VPN Client does not recognize this. The VPN Client still tries to connect to a backup server, and gets hung up about it.

Users see the following log messages:

```
188    13:59:06.623  11/23/04  Sev=Info/4CM/0x63100024
Attempt connection with server ""

189    13:59:06.663  11/23/04  Sev=Info/6IKE/0x6300003B
Attempting to establish a connection with 0.0.0.0.

190    13:59:07.705  11/23/04  Sev=Warning/2CVPND/0xA3400018
Output size mismatch. Actual: 0, Expected: 237. (DRVIFACE:1341)

191    13:59:08.806  11/23/04  Sev=Warning/2CVPND/0xA3400018
Output size mismatch. Actual: 0, Expected: 237. (DRVIFACE:1341)
```

Caveats Resolved in VPN Client for Windows, Release 4.6.00.0045

Release 4.6.00.0045 is the first VPN Client 4.6 release.

This list is based on issues resolved independent of the Cisco VPN Client Release 4.0.4.D software. Refer to the release notes for Release 4.0.4.D for additional caveats resolved since Release 4.0.

Release 4.6.00.0045 resolves the following issues:

- CSCee32555
Microsoft had made a change in Windows XP SP2 beta1 that was incompatible with the Cisco VPN Client. After our conversations, Microsoft has decided to remove the incompatible changes from the final release of Windows XP SP2. Customers should upgrade to the final release of Windows XP SP2 when available.
- CSCee68027
When the user is allowed to put a password on a User Certificate, the 4.6 Beta CLI certificate manager allows invalid passwords to be matched. This happens on all platforms.
- CSCef44186
If you are using IPSEC over TCP, the VPN Client does not work with Windows XP SP2.
- CSCef52730
Windows AutoUpdate dialup cannot uninstall while dialed up. While attempting to AutoUpdate a Windows VPN Client over dialup on Windows XP, error 28004 appears. Remote dialup connections should be disabled prior to uninstalling the client.
Workaround:
When prompted with an OK box notifying the user that a previous client is about to be uninstalled, the user should disconnect all dialup connections.
- CSCeh63357
When installing the VPN Client using a chained MSI, vpnclient.exe and qtwidgets.exe do not have a short path defined. This causes the install to fail.

Caveats Resolved in VPN Clients for Linux

The following sections list the resolved caveats for each release of the 4.6.x.y Linux VPN Client.

- [Caveats Resolved in VPN Client for Linux, Release 4.6.03.0190, page 75](#)
- [Caveats Resolved in VPN Client for Linux, Release 4.6.02.0030, page 76](#)

Caveats Resolved in VPN Client for Linux, Release 4.6.03.0190

- CSCeh17709
When using the ForceNetLogin feature the icon tray does not have a VPN icon. This happens with all ForceNetLogin connections.
- CSCeh39564
The message “ppp0: non-ether hw address (512)” appears during the Linux VPN Client connection. This appears only with PPP connections. It has no effect on the functioning of the VPN Client
- CSCeh41571
Over ISDN, the Release 4.6.02.0030 Linux VPN Client fails to pass traffic.
- CSCeh53258
The Linux VPN Client does not install. It gives the following messages:

```
#error Invalid kernel header included in userspace  
#warning Using kernel header in userland program. BAD!
```
- CSCeh65770
Connectivity is lost when the Linux VPN Client is connected (4.6.02.0030 and higher). Some Linux distributions have the `rp_filter` enabled. The new VPN Client Virtual Adapter interferes with this setting while connected and may result in a loss of connectivity.
- CSCeh74933
When using the Release 4.6.02.0030 Linux VPN Client with Virtual Adapter, the VPN Client no longer passes traffic through the tunnel. If the mask pushed from the VPN 3000 Concentrator for the Virtual Adapter overlaps the host

address of the Concentrator, the Client cannot pass traffic. By default, the Concentrator pushes the classful mask of the network if the mask is left at 0.0.0.0 in the configuration of the Concentrator.

Caveats Resolved in VPN Client for Linux, Release 4.6.02.0030

- CSCee27420
The Linux VPN Client does not work with DNS requests and SMTP.
- CSCee60160
The Linux VPN Client will not work properly with the tg3 Ethernet driver. The tg3 driver is a new Linux driver that has not yet had all of its own issues resolved.
- CSCef38768
A machine running Cisco Linux VPN Client, Version 4.0.5, displays the following message in the kernel log (and subsequently in syslog):
Error: Badness in local_bh_enable at kernel/softirq.c:136
This message did not appear using either version 4.0.4 or 4.0.3. This is experienced with Kernel 2.6.7-gentoo- r8.
- CSCef96957
When attempting to use a SecurID token card with the Linux or Solaris 4.6 VPN Client, the client fails with a segmentation fault.
This occurs only if the token card is doing New PIN Mode and is using the SecurID server to generate the new PIN. If the user creates the new PIN, then the fault does not occur.
- CSCeg59031
If the Linux VPN Client with Virtual Adapter fails, the routing table does not recover back to its original state. The routing table is left as it was when the VPN Client was connected and must be recovered manually at this time. Performing “vpnclient connect” and “vpnclient disconnect” does not recover the proper routing.

- CSCeg59043

The Linux VPN Client with Virtual Adapter fails to connect over PPP, PPPoE, and ISDN connections. All Point-to-Point connections fail because these interfaces have no MAC address. Wireless Ethernet works because the wireless card has a MAC address.

- CSCeg82216

Linux VPN Client with Virtual Adapter 4.6.01.x loses connectivity after DHCP renewal. The routing of the VA prevents proper renewal and a DHCP Discover packet breaks the VPN Connection (Duplicate of CSCeh28264).

- CSCeh21235

When using the Linux VPN Client with Fedora Core 3 2.6.10 or higher, the Client does not install. Compile errors are produced during the installation of the Client because checksum offloading is enabled in the kernel.

- CSCeh28264

When using the Linux 4.6.02 VPN Client, the tunnel disconnects at every DHCP renewal. The DHCP server is not on the same network as the workstation (Duplicate of CSCeg82216).

- CSCsa50543

Installing the Linux VPN Client, you might see the following error messages during the install:

```
/root/vpnclient/interceptor.c: In function `add_netdev':
/root/vpnclient/interceptor.c:59: sorry, unimplemented: inlining
failed in call to 'supported_device': function body not available
/root/vpnclient/interceptor.c:245: sorry, unimplemented: called
from here
make[2]: *** [/root/vpnclient/interceptor.o] Error 1
make[1]: *** [_module_/root/vpnclient] Error 2
make[1]: Leaving directory `/usr/src/linux-2.6.9'
make: *** [default] Error 2
Failed to make module "cisco_ipsec.ko".
```

This has occurred when installing the 4.6.00.0045 Linux VPN Client on Fedora Core 3. This issue also occurs in the Mandrake distribution 10.1, kernel 2.6.10.

Caveats Resolved in VPN Clients for Solaris

The following sections list the resolved caveats for each release of the 4.6.x.y Solaris VPN Client.

- [Caveats Resolved in VPN Client for Solaris, Release 4.6.02.0030, page 78](#)
- [Caveats Resolved in VPN Client for Solaris, Release 4.6.00.0045, page 78](#)

Caveats Resolved in VPN Client for Solaris, Release 4.6.02.0030

- CSCef26762

When you uninstall the Solaris VPN Client, the contents of `/etc/system` are replaced with a copy of the file captured during the original VPN Client installation. Since another application could have been installed and made its own modifications to the `/etc/system` file, replacing it with an earlier version may disable the application.

- CSCeg44345

When using VLANs or interface numbers greater than 20, the following message may appear when using the Solaris VPN Client:

```
Could not attach to driver. Is kernel module loaded? The
application was unable to communicate with the VPN sub-system.
```

Interfaces were only anticipated to be numbered in the 0-20 range and any interface such as a VLAN configured `ce202000` exceeds that range and is not bound to by the VPN Client.

Caveats Resolved in VPN Client for Solaris, Release 4.6.00.0045

There are no resolved caveats in this release.

Caveats Resolved in VPN Clients for Mac OS X

The following sections list the resolved caveats for each release of the 4.6.x.y Mac OS X VPN Client.

- [Caveats Resolved in VPN Client for Mac OS X, Release 4.6.04.0150, page 79](#)
- [Caveats Resolved in VPN Client for Mac OS X, Release 4.6.04.0061, page 79](#)
- [Caveats Resolved in VPN Client for Mac OS X, Release 4.6.03.0160, page 81](#)
- [Caveats Resolved in VPN Client for Mac OS X, Release 4.6.02.0023, page 81](#)

Caveats Resolved in VPN Client for Mac OS X, Release 4.6.04.0150

- CSCeh93891

When using a large number of split or excluded networks with Mac OS X 10.4, the VPN Client GUI may fail to pass traffic or respond to disconnect or quit. This happens only with the GUI on Mac OS X 10.4 and not on 10.3.

- CSCei10213

After making a VPN Client connection on Mac OS X 10.4, the proxy information configured on the adapter is ignored. The VPN Client ignores the proxy information only on Mac OS X 10.4. Mac OS X 10.3 does not change this information.

- CSCei44596

When connecting with Mac OS X 10.4 and using Classic Applications with the VPN Client, traffic fails to pass through the application. A change in OS X 10.4 causes the pushed DNS of the concentrator to interfere with the operation of the Classic environment. OS X 10.3 does not have this issue.

Caveats Resolved in VPN Client for Mac OS X, Release 4.6.04.0061

- CSCdt41308

You may see a problem with FTP file transfers over a long period of time (hours) while connected with the VPN Client. The symptom is that the FTP session never starts (no response to the 'open' command) and the VPN Client Log Viewer shows the following events:

```
74      22:31:08.704  02/08/01  Sev=Warning/2IPSEC/0xE370000C
```

```
Failed to acquire a TCP control resource, the queue is empty.  
75      22:31:08.704 02/08/01 Sev=Warning/2IPSEC/0xA370001A  
VRS processing failed, discarding packet.  
L
```

Other applications such as PING, HTTP should work fine, but for FTP to work again, you must disconnect and reconnect the VPN Client.

- CSCee71948
Reinstalling or upgrading the Mac OS X VPN Client replaces the vpnclient.ini file.
- CSCeh90822
The Mac VPN Client on a dual processor machine panics when disconnecting the VPN Client with OS X 10.4. Traffic must be passing through the Client when disconnected. This is an intermittent timing problem that occurs 25% of the time when conditions are met. This problem does not appear on single processor machines.
- CSCeh90939
The Mac OS X VPN Client will not remain connected overnight. The VPN Client failed an IKE or IPSec rekey.
- CSCeh92574
While using AFP shares between Mac workstations through a VPN Client tunnel, the workstation panics. This problem occurs only on Mac OS X 10.4.
- CSCeh93569
After installing the Release 4.6.03.0160 VPN Client on a Mac OS X 10.4 system, the Client can connect but not pass traffic, disconnect, or quit the VPN Client. If the user had a previous version of VPN Client installed on 10.3 when they “upgraded” to 10.4 and installed the new VPN Client, they experience this issue.
- CSCeh96683
After making a successful connection with the 4.6.03.0160 Mac VPN Client on Mac OS X 10.4, no traffic passes, and the user cannot disconnect. Force Quit is required to kill the VPN Client. A particular VPN Concentrator configuration in the group is causing this issue. This is a VPN Client bug that exists only when using Mac OS X 10.4.

Caveats Resolved in VPN Client for Mac OS X, Release 4.6.03.0160

- CSCeg48152

The Mac OS X VPN Client does not work with Mac OS X 10.4. Apple is doing a major overhaul for 10.4 and the current Mac VPN Client and its next release will not work on the upcoming 10.4 OS. All customers dependent on the Mac VPN Client should delay their upgrade until we have posted a compatible Mac VPN Client for OS X 10.4.

**Note**

Dual processor workstations do not yet have a stable VPN Client version available that will work with Mac OS X 10.4.

Caveats Resolved in VPN Client for Mac OS X, Release 4.6.02.0023

- CSCeb37161

Using the Mac OS X VPN Client, Release 4.0 or higher, a profile using certificates works fine with the Command Line Interface client, but fails to connect with the VPN Client GUI. The Release 4.0 VPN Client fails to connect, while the Release 4.0.1.A VPN Client warns that the certificate cannot be found. The VPN Client GUI requires the “CertSubjectName” field to be filled out in the profile when using certificates. The CLI does not fill in this line or require it.

Workaround:

Using the GUI, modify the profile and select the proper certificate and save the profile. This fills in the GUI required “CertSubjectName” field. Initially, creating the certificate profile in the GUI also bypasses this issue.

Documentation Updates

The following VPN Client documentation has been updated for Release 4.6. 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*

VPN Client does not support Windows NT, 98, and ME.

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. 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.

© 1999-2011 Cisco Systems, Inc. All rights reserved.