



# Release Notes for Cisco VPN Client, FIPS-Compliant Release 5.0.06-FIPS

---

Updated May 22, 2010

Part no. OL-20925-04

[Introduction](#)

[Changes to Platforms Supported by this Release, page 2](#)

[System Requirements, page 2](#)

[Limitations of the FIPS Release, page 3](#)

[Licensing Requirements for the FIPS-Compliant VPN Client, page 3](#)

[Installation Notes, page 3](#)

[Advisories for Windows 7 and Vista Users, page 5](#)

[Usage Notes, page 6](#)

[Open Caveats, page 15](#)

[Resolved Caveats, page 17](#)

[Documentation Updates, page 19](#)

[Related Documentation, page 20](#)

## Introduction

These release notes are for the Cisco FIPS-compliant VPN Client, Release 5.0.06-FIPS, which features support for Microsoft Windows 7 (32-bit only).



**Note**

---

The Cisco FIPS-compliant VPN Client is based on the Cisco VPN Client, Release 5.0.06. If you *do not* require FIPS compliance for your organization, please download the standard release of the Cisco VPN Client.

---



---

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

The Federal Information Processing Standard (FIPS) 140-2 is a U.S. government standard for specific security requirements for cryptographic modules. This standard applies to all federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems.

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).

This document identifies the system requirements, limitations and restrictions, caveats, and related documentation. Please read it carefully prior to installation. The section, “[Usage Notes](#),” describes interoperability considerations and other issues you should be aware of when installing and using the VPN Client. Where applicable, caveat identifiers appear in parentheses following new feature descriptions and usage notes.

## Changes to Platforms Supported by this Release

VPN Client 5.0.06 features support on Microsoft Windows 7 (32-bit only).

This release does not support Tablet PC 2004/2005 and Microsoft Windows 2000.

## System Requirements

VPN Client 5.0.06 supports the following Microsoft OSs:

- Windows 7 (32-bit only)
- Windows Vista (all released 32-bit versions)
- Windows XP (32-bit)

VPN Client does not support the Tablet PC 2004/2005; and Windows 2000, NT, 98, and ME.

Cisco VPN Client supports up to one Ethernet adapter and one PPP adapter.

VPN Client 5.0.x is incompatible with the combination of Cisco Unified Video Advantage 2.1.2 and McAfee HIPS Patch 4 Build 688. To avoid system failures, uninstall either of these two applications, upgrade McAfee to the latest version, or use VPN Client 4.6.x.

To install the VPN Client, you need

- Pentium<sup>®</sup>-class processor or greater
- Microsoft TCP/IP installed. (Confirm via Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 50 MB hard disk space.
- 128 MB RAM  
(256 MB recommended)
- Administrator privileges

The VPN Client supports the following Cisco VPN devices:

- Cisco Series 5500 Adaptive Security Appliance, Version 7.0 and later.
- Cisco VPN 3000 Series Concentrator, Version 3.0 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.

## Limitations of the FIPS Release

This FIPS release of the Cisco VPN Client has the following limitations:

- Transforms—The FIPS Client only allows AES (128, 192, 256) and SHA-1 transforms.
- Certificates—The FIPS Client only supports certificates that use AES and SHA-1 signatures. The release only supports certificate functionality with the Microsoft CAPI certificate store and *does not* support any certification functionality that uses the Cisco certificate store. In addition, the Certificate tab of the Client GUI and its menu has been removed and does not appear to users.

## Licensing Requirements for the FIPS-Compliant VPN Client

The Cisco FIPS-compliant VPN client is licensed based on the ASA 5500 Series Adaptive Security Appliance model. Each security appliance model requires a different license. The license does not affect the number of allowed concurrent VPN sessions.

The following table shows the Product numbers (also called SKUs) of the licenses for each security appliance model:

Product Number (also called SKU)	Security Appliance Model	Description
ASA-FPS-CL-5510=	ASA 5510	FIPS-compliant VPN Client License
ASA-FPS-CL-5520=	ASA 5520	FIPS-compliant VPN Client License
ASA-FPS-CL-5540=	ASA 5540	FIPS-compliant VPN Client License
ASA-FPS-CL-5580=	ASA 5580	FIPS-compliant VPN Client License
ASA-FPS-CL-5505=	ASA 5505	FIPS-compliant VPN Client License
ASA-FPS-CL-5550=	ASA 5550	FIPS-compliant VPN Client License



### Note

Each new security appliance model purchased after August 31st, 2009 requires a FIPS-compliant VPN client license. Cisco customers with current SMARTnet contracts who purchased an ASA 5500 Series Adaptive Security Appliance before August 31st, 2009 are not required to purchase a license for these specific appliances and may contact the Cisco TAC for information on upgrade rights for the FIPS-compliant VPN client.

## Installation Notes

Refer to the *Cisco VPN Client User Guide for Windows*, Chapter 2, for complete installation instructions for Windows users.



### Note

Due to issues surrounding network installation, Active Directory Group Policy software deployment is no longer supported. For more information and a workaround, refer to open caveat CSCse00525.

## Installation Notes - Windows Platforms

Please consider the following installation considerations for Windows users:

### Avoiding Vista Problems with the TCP/IP Registry Compatibility Service and the VPN Virtual Adaptor

To avoid problems with the TCP/IP Registry Compatibility service and the VPN Virtual Adaptor, we strongly recommend that Windows Vista users install Vista SP2.

For more information about a previous hotfix for this problem, go to this URL:

<http://support.microsoft.com/kb/952876>

### Upgrading from Windows XP Requires a Clean Installation

After upgrading Windows XP to Windows 7 or Vista, one experiences various problems with the VPN Client, ranging from client not logging, client won't connect, virtual adapter not installing, and so on. Upgrading from clean install of Windows XP to Vista has been tested and the VPN Client does work in this situation.

However, upgrading a Windows XP installation with legacy applications ranging from Firewalls, Antivirus, device drivers, and so on, to Windows 7 or Vista is not supported, because the problems stem from the legacy, applications no longer supported by the OS.

### Installing the VPN Client Software Using the MSI Installer

You can use the MSI installer on Windows 7, Vista, and XP. Installing with MSI requires Administrator privileges.

Before installing the Windows MSI installation package, you must manually uninstall the previous VPN Client if it is older than Release 4.7. The MSI installer does not uninstall the older versions; it attempts to install before aborting gracefully. Once a version 4.7 MSI package has been installed on Windows XP, future client versions can detect the release present and automatically begin the uninstallation process.

### Upgrading the VPN Client Software on Windows 7 and Vista

For Windows 7 and Vista, please use add/remove programs to uninstall the VPN Client before upgrading to a new Client release.

## Using the VPN Client

To use the VPN Client, you need:

- Direct network connection (cable or DSL modem and network adapter/interface card), or
- Internal or external modem

To connect using a digital certificate for authentication, you need a digital certificate signed by one of the following Certificate Authorities (CAs) installed on your PC:

- Entrust Technologies ([www.entrust.com](http://www.entrust.com))
- Netscape ([www.netscape.com](http://www.netscape.com))
- Verisign, Inc. ([www.verisign.com](http://www.verisign.com))

- Digital certificate stored on a smart card (supported only on Windows Vista and XP at this time). The VPN Client supports smart cards via the MS CAPI Interface.

The VPN Client accepts a blank password for certificate retrieval, but should not.

## About Version Numbers

VPN Client software uses an all-numeric version numbering system 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, 5.0.01.06000 represents feature release 5.0.01, build 600.

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.

When referring generically to the VPN Client software (that is, without regard to a particular platform or 5.0.x release), these release notes use the term VPN Client.

## Advisories for Windows 7 and Vista Users

Windows 7 and Vista users should be aware of the following characteristics of the AnyConnect Client.

### Connection Time

Using the VPN Client to connect a PC running Windows 7 or Vista system might take longer than one running Windows XP. The actual time it takes to connect might vary from customer to customer.

### Unsupported Features

The Cisco VPN Client for Windows 7 and Vista does *not* support the following features:

- Upgrade from Windows XP (clean OS installation required).
- Start Before Logon
- Integrated Firewall
- InstallShield
- 64-bit support

For x-64 support, customers should explore with their Cisco sales representative the use of the next-generation Cisco AnyConnect VPN Client.

- AutoUpdate
- Translated Online Help - Provided only in English



### Note

Cisco VPN client now supports smart card authentication on both Windows Vista and XP. Due to a lack of availability of Windows 7 smart card drivers at release time, Cisco has not yet performed validation testing of smart cards on Windows 7.

# Usage Notes

This section lists issues to consider before installing VPN Client Release 5.0.06.

In addition, you should be aware of the open caveats regarding this release. Refer to “Open Caveats” on page 15 of these Release Notes for the list of known problems.

**Note**

Support for this release is provided through the Cisco TAC for customers with SMARTnet support contracts.

## Split DNS with Wildcards

A split-dns value containing wildcards can cause a system failure when a Windows user accesses certain URLs. For example, the split-dns value a,b,c,d,e,f,g,h,i,j,k,l,m,no,p,q,r,s,t,u,v,w,x,y,z can cause a system failure. To avoid these failures, move the VPN adapter to the top of the binding order list of network adapters. Note that Split DNS requires entries only for internal domains.

## Potential 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.

### Windows Interoperability Issues

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

#### Microsoft Internet Connection Sharing Incompatible

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

#### VPN Client Cannot Launch Microsoft Connection Manager

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

#### 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 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 must enter the fully qualified domain name of the host that needs to be resolved.

## Network Interfaces

- The VPN Client does not support Point-to-Point Protocol over ATM (PPPoA).
- The VPN Client cannot establish tunnels over Token Ring. However, it does not conflict with an installed Token Ring interface.
- The VPN Client on Windows 7 does not support WWAN devices (also called wireless data cards).

## Microsoft Outlook Error Occurs on Connect 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 do *not* experience a problem, do *not* change the MTU value. Usually, an MTU value of 1300 works. If it does not, 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	Use SetMTU.

## Cert DN Matching Cannot Match on Email Field EA

You cannot match the Cert DN field (EA) when using the Peer Cert DN Verification feature on the VPN 3000 Concentrator because the VPN 3000 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, the VPN dialer application loads during a shutdown or restart of the operating system. This does 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, 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 (CSCdy45351).

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

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

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

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

## 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, errors similar to the following occur when the PC boots:

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 records a message similar to the following:

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

The result of such errors is that the ZoneAlarm GUI does not run, and therefore a user cannot change any settings in ZoneAlarm Plus or allow new programs to access the Internet. (CSCdy16607).

## CheckPoint ZoneAlarm (Integrity Agent) Is Incompatible with VPN Client

The VPN Client is not compatible with the software firewall provided with ZoneAlarm (Integrity Agent) v8.0.298. (CSCtc46109)

## 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. The installation continues. See ZoneLabs’ bug number 10182.

## DHCP Route Renewal

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, 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 7 and Vista, you can increase the metric of the public network as follows:

- 
- Step 1** Select Start > Control Panel > (Network and Internet) > View Network Status and Tasks.
  - Step 2** Right-click the icon representing the public interface and select Properties.
  - Step 3** Select Internet Protocol Version 4 and click Properties.
  - Step 4** Click Advanced in the General tab, and set the interface metric to 2 or greater.
- 

In Windows XP, you can increase the metric of the public network as follows:

- 
- 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.
- 

## Windows XP Only—Data Meant for Private Network Stays Local if VPN Client 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 on 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

Beginning with VPN Client, Release 4.6, the 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 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 (CSCee66180).

## 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.

## 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

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 (CSCec82220).

## Allowing ICMP Traffic to Pass Through the Firewall

The following configurations allow inbound ICMP packets (pings) when the default firewall rule for the Centralized Protection Policy (CPP) is pushed to the VPN Client.

On the VPN Client:

- Stateful Firewall (Always On) is enabled.
- The setting “StatefulFirewallAllowICMP=1” is added to the [Main] section of the vpnclient.ini file.
- A connection is made to the VPN Concentrator that pushes the default CPP firewall rule to the VPN Client.

Use the parameter, “StatefulFirewallAllowICMP=1” only if you want to allow ICMP traffic to pass through the firewall.

## 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 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. The VPN Client log also 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.

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

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

To make a connection with cTCP when the Checkpoint VPN-1 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.
- 

## Installing the VPN Client on a 64-bit Vista Machine Results in a 1721 Error

Cisco IPsec Client does not support 64-bit. If the user requires 64-bit support, the upgrade path is to use the Cisco AnyConnect VPN Client instead, which does support 64-bit. However, the AnyConnect Client supports only SSL VPN connections (CSCsi26069).

For Windows 7 and Vista, there is no firewall support in the VPN Client. To resolve the blue-screen issue on Windows XP related to the VPN client built-in firewall, upgrade to VPN Client version 5.0.5-FIPS or higher.

## Installing the VPN Client on a Japanese System Using MSI

Follow these steps to install the VPN Client on a Japanese system, using Microsoft Installer:

- 
- Step 1** Extract the file vpnclient-win-msi-5.0.00.0340-k9.exe to any folder.
  - Step 2** Execute vpnclient\_setup.msi. The installer runs in English.
  - Step 3** After installation is complete, modify vpnclient.ini as follows: ClientLanguat=jp

**Step 4** Launch the VPN Client.

---

## Duplicate IP Address Triggers Error 442 on Windows 7 and Vista

The following error “Reason 442: failed to enable virtual adapter” appears after Windows 7 and Vista reports a duplicate IP address detected. Subsequent connections fail with same message, but the OS does not report a duplicate IP address detected.

To work around error 442, do the following steps:

---

- Step 1** Open “Network and Sharing Center”.
  - Step 2** Select “Manage Network Connections”.
  - Step 3** Enable the Virtual Adapter (“VA”—Cisco VPN Adapter).
  - Step 4** Right-click on Cisco VPN Adapter and select “Diagnose” from the context menu.
  - Step 5** Select “Reset the network adapter Local Area Connection X”.
- 

If this procedure does not work, run the following command from cmd:

```
reg add HKLM\System\CurrentControlSet\Services\Tcpip\Parameters /v ArpRetryCount /t  
REG_DWORD /d 0 /f
```

Then reboot.

This resolves the issue until the OS reports a duplicate IP address again. Follow the preceding steps to resolve it again.

If that doesn't work, you might have UAC enabled. If so, you must run cmd as administrator and repeat the previous registry workaround.

## Windows 7 and Vista Window Auto-tuning Feature Might Cause Network Timeout Problems

Windows 7 and Vista support a feature called “Receive Window Auto-Tuning” that continually adjusts the receive Windows size, based upon the changing network conditions.

Some people reported that auto-tuning causes network timeout problems with some applications and routers. If you have experienced such problems, you can turn it off using the following procedure:

---

- Step 1** Open an elevated command prompt.
  - Step 2** Enter the following command to disable auto-tuning:  

```
netsh interface tcp set global autotuninglevel=disabled
```
- 

If this does not fix the problem, you can turn it back on, as follows:

- 
- Step 1** Open up an elevated command prompt.
- Step 2** Enter the following command to enable auto-tuning netsh interface tcp set global autotuninglevel=normal
- To view the states of the TCP global parameters, use the following command:
- ```
netsh interface tcp show global
```
- (CSCsi26106)
- 

## Windows Vista Error 412

When running under Windows Vista, you might encounter error 412: The remote peer is no longer responding.

To work around this error, upgrade the local NAT device firmware. If this is not possible, switch to TCP. If switching to TCP is not possible, use the following keyword in the connection profile (\*.pcf):

```
UseLegacyIKEPort=1
```



### Note

If you are using Domain Isolation, you cannot use the UseLegacyIKEPort keyword, as this conflicts with Microsoft Domain Isolation.

---

## Open Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The open caveats with Severities 2 and 3 in both Cisco VPN Client Releases 5.0.06.0111 and 5.0.06.0161 are:



### 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, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to [http://www.cisco.com/cgi-bin/Support/Bugtool/launch\\_bugtool.pl](http://www.cisco.com/cgi-bin/Support/Bugtool/launch_bugtool.pl).

---

- CSCec02663

On Windows Vista Ultimate, the Auto Initiation feature fails when the PC is booted up. If the user manually launches the VPN Client, Auto Initiation takes place. This issue does not affect Windows XP Pro.

- CSCsi25985

Vista: User is not prompted to reconnect or cancel after sleep or hibernation while the client is connected. Instead, the client is left hanging trying to disconnect.

#### *Workaround*

Close the client interface and reopen it to make connections again.

- CSCsi26020

Vista: The Firewall Tab still exists under the statistics Windows on Vista, even though the Firewall function is not installed.

#### *Workaround*

This tab can be ignored and will be removed if a new SDK is not provided in time for the integrated firewall.

- CSCsi26033

Enabling logging on Windows Vista results in no information being shown in the client UI log window.

*Workaround*

The log information is still being collected and written to the log files in the Logs directory under the client installation directory.

If you open the active log using Notepad, the log information is then viewable in the client UI log window.

- CSCsi26086

After upgrading Windows XP to Vista one experiences various problems with the VPN client, ranging from client not logging, won't connect, virtual adapter not installing, etc.

*Workaround*

Upgrading from clean install of Windows XP to Vista has been tested and the VPN client does work in this situation.

However, upgrading a Windows XP installation with legacy applications ranging from Firewalls, Antivirus, device drivers, etc., to Vista is not supported since the problems are stemming from the legacy unsupported applications on Vista and not from the VPN client.

- CSCsi26159

Vista: bsod during install/uninstall/sleep with active ras.

When installing or uninstalling the VPN client with an active PPP "RAS" connection, Windows Vista-based computers blue-screen with a stop message.

This is related to a bug in Windows Vista-based computers, and Microsoft has provided a hotfix to resolve this.

NOTE: Some mobile broadband cards provided by cellular wireless providers are treated as a PPP "RAS" connection.

The article goes on to state that Vista blue-screens when the computer is put to sleep while there is an active PPP connection.

*Workaround*

Either disconnect the PPP connection before installing or uninstalling the VPN Client or install the hotfix from Microsoft.

For more information regarding this issue, please see:  
<http://support.microsoft.com/kb/931671/>

- CSCsi26229

Vista: integrated firewall not installed on Vista.

When connecting to a group that requires the firewall on Vista, the client terminates the connection due to Firewall policy mismatch.

*Workaround*

Do *one* of the following:

- Disable the firewall check on for that group on the VPN appliance.
- Clear a custom DLL check looking for the Microsoft Firewall DLLS.

- Use an alternative Firewall that is supported on Vista and by the VPN appliance.

CPP pushes do not work for any Firewalls other than ZoneLabs. If or when ZoneLabs releases ZoneAlarm for Vista, customers can install this to get CPP support.

- CSCsi40595

When the VPN Client is connected and web traffic is passed, the system blue screens if a Trend Micro virus application is running. In this case, the application was Trend Micro PC-cillin 2007, (8.32.1003/4.381.50).

*Workaround*

The normal workaround for conflicts with virus agents is to disable the VPN Client's built-in firewall by renaming the following three files and rebooting:

- vsdata.dll
- vsinit.dll
- vsdatant.sys

In this case, the workaround failed, and the issue disappeared only by stopping the following Trend Services:

- Trend Micro Central Control Component
- Trend Micro Personal Firewall

- CSCsh62685

When using IPSEC over TCP between a VPN client installed on a Windows XP machine with integrated XP firewall, it appears that although IKE and IPSEC are established over TCP port 10000, the Windows XP firewall is still blocking incoming IKE traffic (which it seems to be detected over UDP port 500).

This causes incoming IKE DPDs to be dropped, and the connection to be torn down from the headend side.

*Workaround*

Add the following program as an exception for the Windows Firewall:

/Program Files/Cisco Systems/VPN Client/cvpnd.exe

## Resolved Caveats

Cisco VPN Client Release 5.0.06.0161 resolves the following caveats:

- CSCsr08760  
VPN client does not handle IP option properly under Vista.
- CSCtd08761  
PC reboots if physical link is disrupted during a VPN connection.

Cisco VPN Client Release 5.0.06.0111 resolved the following caveats:



**Note**

For interim bug fixes resolved by previously posted releases, reference the readme documents posted with the software.

- CSCsv22636  
When Password management (Radius-to-AD or AD-LDAP) is set up in a tunnel-group or ASDM connection profile, the IPsec Client version 5.0.4.300 presents the New Pin and Confirm Pin prompts.  
Password-mngt/change is carried out OK, however.  
It should present the prompts “New Password and Confirm Password” prompts instead.
- CSCta06006  
The IPsec VPN Client cannot connect using a Digital Certificate with a key size greater than or equal to 1024 bits and when “Send CA Certificate Chain” is also enabled on the client. This occurs with versions as early as 4.8.01.0300 up to 5.0.05.0290.
- CSCsz35825  
With Vista, IKE Phase 1 fails after redirect from VPN cluster IP to cluster member IP.
- CSCta78716  
IPsec Client GUI crashes during the application of <http://support.microsoft.com/kb/956607>. The workaround was to launch the VPN client via the command prompt.
- CSCsz97108  
The VPN Client uninstall sometime locks up (stops) and cannot be canceled. The PC needs to be rebooted and multiple steps must be done to properly remove the client.
- CSCsz46795  
With Split-tunneling disabled, VPN Client Local LAN route pointing to the VPN Adapter is not added to the routing table on client machine.
- CSCsw69455  
When using RADIUS with password expiry, the GUI prompts for a domain but the command line does not, and the command line connection fails.



**Note** See “[domain](#)” Added to “[vpnclient connect](#)” Command, page 19 for information about this fix.

- CSCsw64279  
Users are able to save their password using an exclamation point (!) even though the head end is configured to prevent stored user passwords.
- CSCsw37419  
The VPN client using certificate authentication with a 4096 bit ID certificate fails to connect. The following error messages may be seen in the vpn client log:  

```
Failed to RSA sign the hash for IKE phase 1 negotiation using my certificate.
Failed to generate signature: Signature generation failed (SigUtil:97)
Failed to build Signature payload (MsgHandlerMM:489)
Failed to build MM msg5 (NavigatorMM:312)
```

Unexpected SW error occurred while processing Identity Protection (Main Mode)  
negotiator: (Navigator:2263)

- CSCsx20992

The VPN Client installer fails to install on low-resolution displays such as those with less than 800x600.

## Documentation Updates

Please use this section as a reference to the updates queued for the following guides:

- *Cisco VPN Client Administrator Guide, Release 4.6*
- *Cisco VPN Client User Guide for Windows, Release 4.6*

### Updates to the *VPN Client Administrator's Guide*

Please note the following updates.

#### Windows Support Limited to Windows 7, Vista, and XP

References to Windows operating systems other than Windows 7, Vista, and XP are not valid for this release.

#### Custom MSI Scripts Not Supported

Cisco no longer supports custom MSI scripts, including the oem.mst file referenced in the “Customizing the VPN Client Software” section.

#### “domain” Added to “vpnclient connect” Command

We added the domain option to the **vpnclient connect** command, as follows:

```
vpnclient connect <profile> [user <username>] [eraseuserpwd | pwd <password>]
[domain <domainname>]
```

Specify the Domain keyword last. In most cases with Radius, the Domain field is not used, so it must be NULL, as shown in the following example:

```
vpnclient connect profile-name user name pwd password domain
```

If the domain name is NULL, the GUI prompts the user for one.

#### “vpnclient\_en\_msi” Filename changed to “vpnclient\_setup.msi”

The vpnclient\_setup.msi file has replaced the obsolete file “vpnclient\_en\_msi” with the file “vpnclient\_setup.msi.” This update applies to the “Installing the VPN Client Using the Transform” section.

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

Because of changes to support Windows 7 and Vista, we no longer support the original novsdata.mst MSI transform.

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

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

## Update to the *VPN Client User Guide for Windows, Release 4.6*

All references to Windows operating systems other than Windows 7, Vista, and XP are not valid for this release.

## Related Documentation

- *Cisco Security Appliance Command Line Configuration Guide, Version 8.0*
- *Cisco Security Appliance Command Reference, Version 8.0*
- *ASDM Online Help*
- *ASDM 6.0 User Guide*
- *Cisco AnyConnect VPN Client Administrator Guide*
- *VPN 3000 Series Concentrator Reference Volume I: Configuration, Release 4.1*
- *VPN 3000 Series Concentrator Reference Volume II: Administration and Management, Release 4.1*
- *VPN 3000 Series Concentrator Getting Started, Release 4.1*

---

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

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

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

© 2010 Cisco Systems, Inc. All rights reserved.