



Release Notes for Cisco VPN Client, Release 5.0.00 and Release 5.0.01

These release notes support Cisco VPN Client software, Release 5.0.00.0340 and Release 5.0.01.0600. This release is exclusively for Windows. Please refer to [About Version Numbers, page 5](#) for information about the 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. Where applicable, caveat identifiers appear in parentheses following new feature descriptions and usage notes.

Contents

- [Introduction, page 2](#)
- [System Requirements, page 2](#)
- [Installation Notes, page 3](#)
- [Advisories for Windows Vista Users, page 5](#)
- [New Feature in Release 5.0.00, page 7](#)
- [Security Considerations, page 7](#)
- [Usage Notes, page 7](#)
- [Open Caveats, page 23](#)
- [Resolved Caveats, page 26](#)
- [Documentation Updates, page 29](#)
- [Related Documentation, page 30](#)
- [Obtaining Documentation, page 30](#)
- [Obtaining Technical Assistance, page 32](#)



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

© 2008 Cisco Systems, Inc. All rights reserved.

Introduction

The VPN Client, Releases 5.0.00 and 5.0.01, is an application that runs on a Microsoft® Windows®-based personal computer that meets the system requirements stated in the next section.

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* 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, including Tablet PC	<ul style="list-style-type: none"> • Windows Vista (all released versions) • Windows XP • Windows 2000¹ • TabletPC 2004/2005 <p>Note For all Windows operating systems, only 32-bit platforms are supported.</p>	<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) – 32 MB for Windows 98 (See note under Operating Systems.) – 64 MB for Windows NT and Windows ME (See note under Operating Systems.)
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 <p>Note The VPN Client does not support SMP (multiprocessor) or 64-bit processor kernels.</p>	<ul style="list-style-type: none"> • 32 MB Ram • 50 MB hard disk space

Computer	Operating System	Requirements
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 4.8.x versions supports Mac OS X on Intel processors.

1. The VPN Client supports the both the Windows 2000 Server and the Windows 2003 Server operating systems.

Cisco VPN Client for Windows Vista, release 5.0.0.340, does *not* support the following features:

- System upgraded from Windows XP or earlier Windows operating systems to Vista. (Clean OS installation required.)
- Start Before Logon.
- SmartCard authentication.
- Integrated firewall
- InstallShield.
- Auto Update.
- Translated Online Help. Online Help is provided only in English.

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 (CSCsq87252).
- 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

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.

Files in VPN Client for Windows, Release 5.0.01.0600

The following files are included in VPN Client for Windows, Release 5.0.01.0600:

- vpnclient-win-msi-5.0.01.0600-k9.exe - Windows 2000, XP and Vista - 32bit only.
- update-5.0.01.0600-major-k9.zip - 32bit only.

Files in VPN Client for Windows, Release 5.0.00.0340

The following files are included in VPN Client for Windows, Release 5.0.00.0340:

- vpnclient-win-msi-5.0.00.0340-k9-bundle.exe—Windows client MSI installer
- vpnclient-win-is-5.0.00.0340-k9-bundle.exe—Windows client InstallShield installer
- update-5.0.00.0340-major-K9.zip—VPN Client Auto Update package. Vista does not support Auto Update.

**Note**

Windows Vista requires MSI installation.

Installation Notes - Windows Platforms

Release 5.0.00.0340 and Release 5.0.01.0600 include the following installation considerations for Windows users:

Upgrading from Windows XP to Windows Vista Requires a Clean Installation

After upgrading Windows XP to Windows 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 Vista is not supported, because the problems stem from the legacy, unsupported applications on Vista and not from the VPN client (CSCsi26086).

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.

The InstallShield installer is not part of 5.0.01.0600, so you must use the MSI installer for this release. The VPN Client Installer does not allow installations from a network drive (CSCeb43490).

**Note**

You cannot use InstallShield to install the VPN Client on a PC running Windows Vista. You must use the MSI installer if you are using Windows Vista, because Vista does not support installation using InstallShield.

Installing the VPN Client Software Using the MSI Installer

If you are using the MSI installer, you must have Windows 2000, Windows XP, or any released version of Windows Vista. 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 Release 4.7. The Release 5.0 MSI installer does not detect older versions, and the installer attempts to install before aborting gracefully. Once a version 4.7 MSI package has been installed, future client versions can detect the existing release 5.0.x installation and automatically begin the uninstallation process.

**Note**

Windows Installer 2.0 must be installed on a Windows 2000 PC before configuring the PC for a Restricted User with Elevated Privileges (CSCea37900).

Using the VPN Client

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

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 5.0.

Advisories for Windows Vista Users

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

Connection Time

Using the VPN Client to connect to a Windows Vista system might take longer than the time needed to connect to a Windows 2000 or Windows XP system. The actual time it takes to connect might vary from customer to customer.

Unsupported Features

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

- System upgraded from Windows XP to Vista (clean OS installation required).
- Start Before Logon
- SmartCard Authentication
- Integrated Firewall
- InstallShield
- 64bit support
- AutoUpdate
- Translated Online Help - Provided only in English

New Feature in Release 5.0.01

VPN Client, Release 5.0.01, introduces SmartCard support for Start Before Logon and configurable tunnel trade-in behavior.

**Note**

The Cisco VPN Client for Windows Vista does not support SmartCard authentication.

SmartCard Support for Start Before Logon

In previous versions, SmartCards were supported only after a user had logged in to the system. This enhancement allows SmartCards to operate even when the VPN Client is operating in SBL mode (CSCsb73913).

Configurable SmartCard Teardown Behavior

By default, Cisco VPN remote access software clients (both IPSec and SSL) tear down existing VPN tunnels when the user removes the SmartCard used for authentication. Beginning with ASA Release 7.2 or later, the central-site administrator can override this client behavior for the duration of the tunnel.

The administrator can configure whether to preserve or tear down a VPN tunnel when a SmartCard is removed and pass the value indicating whether to tear down or leave up the tunnel to IPSec client.

During IKE negotiation, the security appliance performs a group/user lookup. As part of this lookup, the SmartCard Removal Disconnect attribute is requested from the authentication database. The value of this attribute is then sent to IPSec clients under the identity of the Mode Config attribute, but this attribute is sent only to clients that request it. Older clients that do not request or support this attribute are not affected. In addition, older VPN 3000 Concentrator and ASA 5500 central-site devices ignore requests for this attribute from newer clients, since these devices do not support this feature.

You configure the client action for SmartCard removal as part of configuring group policy, using the **smartcard-removal-disconnect** command:

```
group-policy name attributes
  [no] smartcard-removal-disconnect {enable | disable}
```

Disabling this option configures the Client to leave existing tunnels connected when a SmartCard is removed. Enabling this option configures the Client to disconnect existing tunnels when a SmartCard is removed. This option is enabled by default. The **no** form of the command removes the command from the configuration and reverts to the default value(CSCsh05659, CSCsi71041, CSCsi72400).

New Feature in Release 5.0.00

VPN Client, Release 5.0.00, introduces support for Windows Vista.

Security Considerations

The feature called “Allow launching of third party applications before logon”, (Start Before Logon), which is available through “Windows Logon Properties” in the VPN Client Options menu, has security implications that system administrators must be aware of.

When this option is enabled, the VPN Client dialer launches an application before establishing a connection from the Windows logon screen. The specific application that is launched can be selected by the user, regardless of the user's privilege level. Because the selected application is launched from the Windows logon screen, before any user has logged into Windows, the application runs with the privileges of the LocalSystem account, which has administrative privileges. This makes it possible for unprivileged users to elevate their privileges to those of the LocalSystem account if the “Allow launching of third party applications before logon” feature is enabled.

For this reason, “Allow launching of third party applications before logon” is a privileged option that can be enabled only by the system administrator. If this option is greyed out in the VPN Client graphical user interface, then users cannot launch applications and third-party dialers before logging on to a Windows machine. However, once this option is enabled, there is a potential for local privilege escalation that system administrators must be aware of.

Cisco does not recommend the use of the “Allow launching of third party applications before logon” feature if users are not allowed administrative access to their Windows machines.



Note

All these security considerations apply to all VPN Client versions and to all supported Windows operating systems, with the exception of Windows Vista (which does not support the Start Before Logon feature).

Usage Notes

This section lists issues to consider before installing Release 5.0.00 or 5.0.01 of the VPN Client software.

In addition, you should be aware of the open caveats regarding this release. Refer to “Open Caveats” on page 23 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.

Advisory:

With VPN Client Release 5.0.2 and higher, users can upgrade from an IS-based installation to MSI without having to first manually remove the IS package (CSCsk37470).

The Cisco VPN Client for Windows Vista does NOT support the following:

- * System upgraded from Windows XP to Vista (clean OS installation required).
- * Start Before Logon
- * SmartCard Authentication
- * Integrated Firewall
- * InstallShield
- * 64bit support
- * AutoUpdate
- * Translated Online Help - Provided only in English

Establishing a connection on Vista takes longer compared to XP. This is not a bug and is due to additional processes Vista goes through when an adapter is enabled.

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.

**Note**

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

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 (CSCdx85663).

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 token 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 (CSCdv47999). 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 (CSCdv65165).

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.

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 (CSCdv67594).

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 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	<p>Windows XP and Windows Vista</p> <p>Use SetMTU</p>
PPPoE - EnterNet	<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 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></p> <p>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 (CSCdu80463).</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 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 (CSCdt10266).

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 (CSCdx25994).

VPN Dialer Application Can Load During OS Shutdown or Restart

When using the VPN Client's Start Before Logon feature (Windows 2000 or Windows XP) 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 (CSCdu02071).

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, Vista), 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 (CSCea29056).

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 on 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 on 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, upgrade to Internet Explorer v5.0 or greater (CSCdv70215).

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, or higher, and your PC must have Internet Explorer version 5.0 SP2 or later installed to function properly. (CSCdx90228).

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” (CSCdu25495).

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 (CSCdu29239).

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 (CSCdu33638).

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 (CSCdu61926).

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, you see a prompt 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 (CSCdu62212).

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 (CSCdu84038).

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 (CSCdy14238).

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.(CSCdy16607).

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 (CSCea25991). See ZoneLabs’ bug number 10182.

DHCP Route Renewal in Windows 2000 and Windows XP

In a Windows 2000, Windows XP, or Windows Vista 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 (CSCdz88896). 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.
-

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 (CSCdz38680).

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 (CSCee66180).

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 (CSCdy62426):

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

```
Driver_IRQL_Not_Less_Or_Equal
```

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

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 (CSCdy87504). 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 (CSCea03349).

Downgrading VPN Client from Release 4.8 Causes Start Before Logon Failure

Do we really still need this one? Does this also apply to 5.0.x?

Start Before Logon fails if the VPN Client is downgraded from Release 4.8 to 3.6. The reason for this is that the file `csgina.dll` is upgraded when the VPN Client version 4.8 is installed. If the VPN Client is downgraded to version 3.6, the `csgina.dll` file for version 4.8 is not replaced, and this breaks ability in the VPN Client version 3.6 to Start Before Logon (CSCea03685).

Follow this procedure to drop back to the VPN Client version 3.6 from version 4.8.

-
- Step 1** Uninstall the VPN Client version 4.8.
 - 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 (CSCdz52156).

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 (CSCec82220).

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 (CSCec79691).

Allowing ICMP Traffic to Pass Through the Firewall

The following configuration s 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 (CSCdz87487).

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. 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 (CSCea66549).

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) (CSCea16012).

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 (CSCea43117):

<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 Secureremote 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 Secureremote is installed, you must disable the Check Point SecuRemote driver in the Connections Properties. To do this, you must be administrator. Follow these steps (CSCea31192):

-
- 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. Note that the AnyConnect Client supports only SSL VPN connections (CSCsi26069).

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.
-


Note

A new MST has been published on Cisco.com to resolve the issue for the Japanese installation (CSCsi02975).

Duplicate IP Address Triggers Error 442 on Windows Vista

The following error “Reason 442: failed to enable virtual adapter” appears after Vista reports a duplicate IP address detected. Subsequent connections fail with same message, but Vista doesn't 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 REGDWORD /d 0 /f
```

Then reboot.

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

If that doesn't work, run the following from cmd.

**Note**

If you have UAC enabled, you must run cmd as administrator:

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

(CSCsi26106)

Vista Window Auto-Tuning Feature Might Cause Network Timeout Problems

Vista introduces a new 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)

s

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 following lists are sorted by identifier number. Support for this release is provided through the Cisco TAC for customers with SMARTnet support contracts.



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.

- 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 and Win 2000 SP4.

- CSCsb05686

VPN Client fails to add routes to the routing table. This happens only when the nw adapter has more than 1 IP address attached to it. Otherwise it works fine.

Workaround

Don't add secondary IP address to the network adapter that is used for VPN connectivity.

- CSCsi25954

Vista: Certificate authentication via SmartCards are not supported.

When connecting to a profile that requires certificate authentication and the certificates are stored on a SmartCard, Vista prompts the user to allow the client service to interact with the desktop. After the user enters the PIN and closes the alternative desktop, the client service is left hanging and unresponsive.

Workaround

Reboot the client machine or enter the “net stop cvpnd” and then “net start cvpnd” commands to get the client working again.

To use certificate based authentication, the certificate must be exported from the SmartCard and imported into the Cisco Certificate Store. Care needs to be take in retaining the certificates PIN when importing the certificate into the Cisco Certificate Store via the client interface.

- 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.

- CSCsi26050

Vista: The InstallShield package does not work on Vista. Attempting to use the InstallShield package on Vista results in an error stating that InstallShield is not supported and to use MSI package instead.

Workaround

Use the MSI package on Vista. The InstallShield package is not supported on Vista.

Any users who are still using the InstallShield package, even on Windows XP, should migrate way from InstallShield and use MSI going forward.

- CSCsi26086

After upgrading Window 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 Bluescreen 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 bluescreens 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, CSCsf07334

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.

- CSCsi35107

Unable to find the SBL configuration settings in the GUI for Vista.

Workaround

Vista does not support the XP-style GINA, therefore SBL has been removed. Until the code has been rewritten in PLAP, configure the client to use Force Net Logon to achieve similar functionality.

When the user connects, the VPN Client logs the user off but keeps the tunnel up. When the user logs back in, the user is authenticating against Active Directory and receives any pushes from AD.

- CSCsi88243

Using the 5.0.00.0340 VPN Client version, if the user's password has expired, the head end does not prompt for the new password on the VPN Client.

This can also happen if the VPN Client needs to set the PIN number or provide the next token code when using, for example, RSA SecurID authentication.

- 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

The following sections list the caveats resolved in the Cisco VPN Client, Release 5.0.xx Resolved caveats are listed in ascending alphanumeric order.

Caveats Resolved in VPN Client, Release 5.0.01.xxxx

- CSCsb73913
 Presently Smartcards are only supported after a user has logged in to the system. This enhancement would allow Smartcards to operate even when the VPN Client is operating in SBL mode.
- CSCsc93119
 IKE pre fragmentation is not working with VPN client 4.0.5.D and above. It does work with VPN Client 4.0.3.F. It appears that IKE fragmentation on the Cisco VPN client 4.0.5.D is broken for UDP, and fragmentation at IP level is used instead, this works correctly with VPN client version 4.0.3.F. VPN Client versions 4.6 and 4.7 show the same behavior as 4.0.5.D IKE fragmentation seems to work correctly for TCP encapsulated IKE packets (which are TCP/500), configuring TCP encapsulation could be used as a workaround
- CSCsd86776
 VPN Client does not accept id-certs signed by a CA with validity > 2099. When you verify a certificate selected in the VPN Client under “Certificates” and click Verify, you get an error: Error 32: Unable to verify certificate “.....”
 The selected certificate was signed by a CA whose certificate validity is longer than year 2099.
- CSCsf96588
 VPN Client does not work properly after waking Laptop up from suspend mode. If a VPN 4.8 Client is connected to a central site-device, and the client device (typically a laptop) goes into Suspend Mode, then the VPN Client disconnects. Upon waking up from Suspend Mode, the VPN Client is disconnected. A pop-up message appears, allowing you to reconnect the VPN connection. However, selecting reconnect does not re-establish the VPN tunnel.
 This situation occurred with the VPN 4.8 Client installed on a Windows XP Laptop. The client disconnects after going into any hibernate or standby situations.
- CSCsf96628
 VPN Client popup dialog box appears squashed, and it moves to the upper left of the screen after a Laptop is woken up from suspend mode (after going into any hibernate or standby situations). This occurs with the VPN 4.8 Client installed on a Windows XP Laptop.
- CSCsg41133
 With multiple smart cards, removal of any card tears down VPN tunnel.
 When using multiple smart cards on a PC, the tunnel is established, but it is torn down if *any* of the smart cards are removed. This is not the intended behavior of the VPN client software.
 The client triggers this error when a card not containing the cert used to connect is removed:

```
329 18:01:38.416 10/13/06 Sev=Info/4 CERT/0x6360002D
Smart card containing active certificate is not found. Terminating connection.
```

This condition occurs when a user has multiple smart cards with certificates in VPN client 4.8.

- CSCsg43468

With multiple smart cards, the user is not re-prompted for PIN to reconnect. The VPN Client always enforces the PIN login prompt when there is only one SmartCard in the PC. However, if there are multiple SmartCards, the user is prompted for a PIN only the first time he or she establishes a VPN connection and is allowed to make further connections without being prompted until the card is disconnected.

- CSCsi39588

Unity Win2k MSI installer pops up dialogs with DLL error messages

Using version 5.0.00.0330, when attempting a fresh install with MSI, the installer pops up the following error dialogs:

- “The procedure entry point GetAdaptersAddresses could not be located in the dynamic link library iphlpapi.dll”
- “Error in custom action. The library C:\DOCUME~1\SYSTEM~1\Temp\{some large string}\insthelper.dll is invalid or could not be found.”

The installer does *not* fail, and it continues to install the Client successfully after these error messages are acknowledged.

- CSCsi26024

Copyright date in “About” windows shows 2006.

Caveats Resolved in VPN Client, Release 5.0.00.0340

The VPN Client for Windows, Release 5.0.00.0340, resolves the following caveats.

- CSCeh97583

When using the CLI syntax `vpnclient connect myProfile user myUser pwd myPassword`, if `myPassword` was mistyped, the password is sent 3 times to the authentication server and fails 3 times. This sometimes locks users out with failed attempts.

- CSCsc74781

Unable to customize the Cisco VPN Client for different languages.

- CSCsd09675

On Vista Beta2, the first time logs are enabled, Microsoft firewall pops up a dialog box to allow the IPsecLog process. To enable logging, please allow IPsecLog process. Log messages do not show up till the log file is touched.

- CSCse39772

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

- CSCse77792

Application crashes when the VPN Client is connected. AES encryption is configured for the VPN Client connection and a VPN Client version of 4.6.01.0019 or higher is in use. The issue is an optimization for the MMX processor introduced by RSA that introduces an error when used with AES.

- CSCsf03420
When using Skype through a VPN Client tunnel, the audio works only in one direction. This happens only when using an AES encryption algorithm. Using 3DES resolves the issue.
The issue is an optimization for the MMX processor that was made by RSA that introduced an error when using AES.
- CSCsh02887
A function is still showing that allows a user to enable the stateful firewall on Windows Vista, even though the integrated firewall is not installed.
- CSCsh12290
Using the Vista Beta client 4.8.01.0590, profiles aren't automatically imported on install when placed in the installation folder. This was introduced by the installer changes for Vista and the MSI installer.
- CSCsh24112
When using VPN client version 4.8.1 on a Windows PC on certain Dell desktops, during the VPN session, sound from the sound card Analog Devices ADI 198x Integrated Audio cannot be heard. This does not happen with Dell laptops using a different sound card.
- CSCsh45583
IPSec client connecting using AES Encryption causes active Windows Media Player 10 playing a local file to fail after connecting. This occurs if Media Player has either SRS WOW or Equalizer enabled. The Media Player incurs High Static to speakers.
This condition occurs under the following conditions: Media Player 10 configured with SRS WOW and/or Equalizer playing local file and then VPN IPSec client connecting to ASA/PIX with AES encryption.
- CSCsi02975
VPN Client Microsoft Installer 5.0.00.0340-MSI.exe can not be installed correctly on Japanese Windows Platforms. Condition: Japanese Windows Vista version 6.0 Build 6000 Japanese Windows XP Professional SP2 Japanese Windows 2000 Professional SP4.

Workaround

Do *one* of the following:

- Use InstallShield 5.0.00.0340-IS.exe on Windows XP or Windows 2000.
- All platforms:
 - a. Extract vpnclient-win-msi-5.0.00.0340-k9.exe to any folder.
 - b. Execute vpnclient_setup.msi. Installer runs in English.
 - c. After installation is complete, modify vpnclient.ini as follows:


```
-----
ClientLanguage=jp
-----
```
 - d. Launch VPN Client; GUI is in Japanese.
- CSCsi26001
Windows XP and Vista: reauth on rekey with saved password causes disconnect. The VPN Client is disconnected when the user has a saved password and reauth on rekey is enabled on the VPN appliance. The previous version of the client did not disconnect the tunnel with a saved password.
- CSCsi50302

Saved password fails on second connection.

- CSCsi62282

RSA securid is not prompting for authentication after first disconnect.

- CSCsi87609

When using the following CLI syntax:

```
vpnclient connect user myUsername pwd myPassword
```

it looks as though the session has hung up. This happens only with the 5.0.00.0340 VPN Client version. It did not happen with prior versions.

A feature added in the 5.0.00.0340 VPN Client version has introduced unexpected side effects. The session is not actually hung up. The connection has been successfully established, but session control has not been returned to the CLI prompt.

Redistributing the Cisco VPN Client

For anyone planning on redistributing the client, please refer to:

http://www.cisco.com/application/pdf/en/us/guest/products/ps5982/c2001/ccmigration_09186a008031f148.pdf,

Section 4 to ensure you comply with Cisco Copyrights and Licenses agreement.

Documentation Updates

The VPN Client documentation is in the process of being updated for Release 5.0, but it is not yet available. The principal changes deal with Windows Vista support. In the interim, please refer to the following documents. The VPN Client documentation was updated for Release 4.6 and did not change for Release 4.7 or 4.8. The following section contains changes to apply to these documents. These documents contain information for all platforms on which the VPN Client runs:

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

VPN Client for Windows, Release 4.6.04.0043 is the final version that supports Windows NT. Earlier versions of Windows (Windows 98, Windows 98 (second edition), and Windows ME) are also not supported.

Documentation Changes

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

Correcting the Obsolete Filename `vpnclient_en_msi`

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

Using MSI to Install the Windows VPN Client without Stateful Firewall

Due to changes to support the Vista platform, the original `novsdata.mst` MSI transform is no longer supported with the VPN Client releases 4.8.02.0010 and higher on Windows 2000, Windows XP, and Windows Vista.

Using InstallShield to Install the Windows VPN Client without Stateful Firewall

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

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

```
DisableFirewallInstall=0/1
```

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

Certificates Exported from Cisco Certificate Store Are in Proprietary Format

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

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*

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

<http://www.cisco.com/univercd/home/home.htm>

You can access the Cisco website at this URL:

<http://www.cisco.com>

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

<http://www.cisco.com/go/subscription>

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpc/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:
<http://www.cisco.com/en/US/partner/ordering/index.shtml>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

Cisco Systems
 Attn: Customer Document Ordering
 170 West Tasman Drive
 San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com, which includes the Cisco Technical Assistance Center (TAC) website, as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from the Cisco TAC website. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC website, including TAC tools and utilities.

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

To obtain customized information and service, you can self-register on Cisco.com at this URL:

<http://tools.cisco.com/RPF/register/register.do>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.

- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

<http://www.cisco.com/tac>

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC website. Some services on the Cisco TAC website require a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

<http://tools.cisco.com/RPF/register/register.do>

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

<http://www.cisco.com/tac/caseopen>

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

<http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml>

Before calling, please check with your network operations center to determine the Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- Cisco Marketplace provides a variety of Cisco books, reference guides, and logo merchandise. Go to this URL to visit the company store:

<http://www.cisco.com/go/marketplace/>

- The Cisco *Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the Cisco Product Catalog at this URL:
<http://www.cisco.com/en/US/products/index.html>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press online at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is no longer published. Cisco is evolving its customer communications to a more interactive, Web-based model, and the company's Website, Cisco.com, has become our primary communications forum to meet the diverse information needs of networking professionals. Follow this link for a list of resources on Cisco.com that may help you in your career:
<http://www.cisco.com/packet>
- *iQ Magazine* is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
- *Internet Protocol Journal* is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:
<http://www.cisco.com/ipj>
- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:
<http://www.cisco.com/en/US/learning/index.html>

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

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website 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. (0705R)

© 2007 Cisco Systems, Inc. All rights reserved.