Release Notes for Cisco VPN Client for Windows, Release 3.5.1

CCO Date: January 30, 2002

Part Number 78-13946-02

These release notes support VPN Client software, Release 3.5.1 and Release 3.5. They describe new features, limitations and restrictions, interoperability notes, caveats, and related documentation. Please read the release notes carefully prior to installation.

Contents

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

Introduction

The VPN Client is a set of software applications that runs on a Microsoft® Windows®-based PC. 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 *VPN Client User Guide* for a complete list of system requirements and installation instructions.

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

- To install the VPN Client, you need
  - CD-ROM drive, or
  - 3.5” high-density diskette drive
  - Administrator privileges (if installing on Windows NT or Windows 2000)
- To use the VPN Client, you need

  - Direct network connection (cable or DSL modem and network adapter/interface card), or
  - Internal or external modem, and
  - For Windows 95, Microsoft Dial-Up Networking (DUN) version 1.2 or greater. (DUN 1.3 for Windows 95 is a recommended performance and security upgrade, and it is available as a free download from the Microsoft Web site, www.microsoft.com. Windows 98 includes the DUN 1.3 function.)

- 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 smart card with a CAPI certificate installed

Installation Notes

Refer to the *VPN Client User Guide* for complete installation instructions. The following notes are important for users who are upgrading to Windows XP and users who want to downgrade to an earlier version of the VPN Client software.

Windows XP Requires VPN Client Release 3.1 or Higher

If you are running Windows XP on your PC, you *must* upgrade your VPN Client to Release 3.1 or higher. VPN Client Release 3.0 does not support Windows XP.

If you are running the VPN Client, Release 3.0, on a PC and you want to upgrade your operating system to Windows XP, you must *first* uninstall the Release 3.0 VPN Client, then install Windows XP, then install Release 3.1 or higher of the VPN Client (CSCdv72593).

Upgrading to Windows XP–Considerations for VPN Client 3.1 and Higher

VPN Client Releases 3.1 and higher *do* support Windows XP, but if you are upgrading to Windows XP, the Microsoft upgrade wizard incorrectly reports that this version of the VPN Client does not support Windows XP, and that you should contact Cisco for an updated version.

To get around this issue, uninstall the VPN Client, upgrade the operating system to Windows XP, then reinstall the VPN Client, Release 3.1 or higher.

New Feature in Release 3.5.1

Release 3.5.1 of the VPN Client software includes the following new feature.

Zone Labs Integrity Firewall Support

The Zone Labs Integrity solution secures remote PCs on Windows platforms. This feature is a client/server solution in which the Integrity Server on a central organization's network maintains policies for the firewall on the remote VPN Client PCs, and the Integrity Agent on the remote PC enforces the policies received from the Integrity Server. The goal is to provide firewall protection while a VPN tunnel is established

Refer to "Personal Firewall Policies" in the next section for a description of support for other firewall features in the VPN Client.

New Features in Release 3.5

Personal Firewall Policies

Release 3.5 enhances the firewall support provided in Release 3.1.

- Integrated Firewall

The VPN Client on the Windows platform includes a stateful firewall integrated within it. This firewall is transparent to the VPN Client user and is called “Cisco Integrated Client Firewall” or CIC.

Note If a session is already active when the Cisco Integrated Client firewall is enabled (either on the VPN Client or by policy pushed down from the VPN Concentrator (CPP), that session is permitted to continue sending outbound packets as long as those packets are not blocked by an outbound rule.

However, if the first packet sent after the firewall is enabled is inbound, the firewall does not allow the packet.

- Support for Centralized Protection Policy or CPP on the VPN Concentrator

  The VPN Concentrator can be configured for CPP (also called “pushed policy”), in which a network administrator can establish firewall rules on the VPN Concentrator and “push” them to the VPN Client.

- Support for local personal firewalls

  In cases where rules are configured on the firewall that resides on the VPN Client PC, the VPN Client polls the firewall every 30 seconds to determine whether the firewall software is still running. This policy is called Are You There (AYT). If the firewall is not running, the VPN Client drops the connection.

Note The minimum supported version of Zone Alarm and Zone Alarm Pro is 2.6.357. If you use a version of Zone Alarm or Zone Alarm Pro that is less than 2.6.357 and you uninstall the VPN Client, the uninstall process removes a file that Zone Alarm or Zone Alarm Pro requires. If this happens, you can correct the problem by reinstalling Zone Alarm or Zone Alarm Pro (CSCdv38365).

Smart Card Support

The VPN Client supports authentication with digital certificates through a smart card or an electronic token. Several vendors provide smart cards and tokens. The VPN Client works only with smart cards and tokens that support CRYPT_NOHASHOID. For a complete description of this feature, refer to the *VPN Client User Guide*.

Datakey CIP Software V.4.6 Works Correctly with VPN Client Release 3.5.1

The Datakey Model 330 32K Smart Card, using CSP (dkrsacsp.dll) version 1.10.141 and CIP software version 4.6 (and higher) is compatible with VPN Client Release 3.5.1 (CSCdw60658).

Documentation Correction Regarding Smart Cards

The table of supported Smart Cards on page 3-12 of the *VPN Client User Guide* contains an error. The entry GEM195 should, instead, be GPK 16000.

Enhanced Login Failure Messages

When the RADIUS with Expiry option is selected on the VPN 3000 Concentrator as the IPSec authentication method for the group, the VPN Concentrator can provide enhanced login failure messages to the VPN Client describing specific error conditions. These conditions are:

- Password expired
- Restricted login hours.
- Account disabled.
- No dialin permission.
- Error changing password.
- Authentication failure.

The “password expired” message appears when a user whose password has expired first attempts to log in. The other messages appear only after three unsuccessful login attempts.

IPSec over TCP

IPSec over TCP encapsulates encrypted data traffic within TCP packets. This feature enables the VPN 3000 Concentrator to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls. This feature does not work with proxy-based firewalls.

To use IPSec over TCP, both the VPN Client (or the VPN 3002 Hardware Client) and the Concentrator to which it connects must be running version 3.5 software.

Compatibility between VPN Client and Double-Byte Character Systems

There are no known issues with the VPN Client operating on a double-byte character system, such as Kanji.

Limitations and Restrictions

This section lists the issues to consider before installing Release 3.5 or 3.5.1 of the VPN Client software. There are no known" limitations and restrictions" unique to Release 3.5.1.

In addition, you should be aware of the open caveats regarding this release. Refer to "Open Caveats, VPN Client Release 3.5.1" on page 20 of these Release Notes for the complete list of known problems.

Potential Application Compatibility Issues

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

Avoiding Extraneous Warnings When Installing the VPN Client under Windows XP

During the VPN Client installation on Windows XP, the following error message appears:

> "The software you are installing for this hardware:
>
> Deterministic Networks Enhancer Miniport
>
> has not passed Windows Logo testing to verify its compatibility with Windows XP."

You are allowed to choose "Continue anyway", but this message pops up a few more times after this. Choose "Continue anyway" until it stops prompting you (which can be as many as 24 times, depending on the configuration). Then the installation continues normally (CSCdu53939).

Before you install the VPN Client, you must do the following to avoid these messages:

Step 1 Select Start | Control Panel | System | Hardware | Driver Signing

Step 2 Set Windows XP Driver Signing to Ignore.

Installing the VPN Client on Windows NT/2000/XP Requires Administrator Privileges

You must have Administrator privileges to install the VPN Client on Windows NT, Windows 2000, or Windows XP because these operating systems require Administrator privileges to bind to the existing network drivers or to install new network drivers.

Allowing the VPN Client to Work Through ESP-Aware NAT/Firewalls

When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client's keepalive implementation, called DPD (Dead Peer Detection). When a Client is idle, it does not send a keepalive until it sends data and gets no response.

To allow the VPN Client to work through ESP-aware NAT/Firewalls, add the following parameter and setting to the [Main] section of any *.pcf (profile configuration file) for the affected connection profile.

ForceKeepAlives=1

This parameter enables IKE and ESP keepalives for the connection at approximately 20 second intervals.

For more information, see “Connection Profile Configuration Parameters” in the *VPN Client Administrator Guide*.

WINS Support

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

Windows NT

Users running Windows NT 4.0 with Service Pack 4 require a hot fix from Microsoft for proper operation. This fix is available on the Microsoft GetHostByName API Returns Unbindable Address page: http://support.microsoft.com/support/kb/articles/Q217/0/01.ASP.

DNS

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

America Online Users (AOL)

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.

Traceroute

The IP traceroute command (TRACERT.EXE) does not work over a secure tunnel. If you have enabled split tunneling, traceroute works over the unencrypted Internet connection.

Incompatibility between VPN Client Microsoft ICS and Sygate Internet Connection Sharing on Windows 98

You cannot install the VPN Client if Windows 98 Internet Connection Sharing (ICS) is already installed on the same Windows 98 system.

Do not install the Sygate ICS application after installing the VPN Client. These two programs do not work correctly on the same Windows system.

The Cisco VPN Client *can* work from behind another PC running ICS by using Transparent Tunneling (Options > Properties > General tab). for information about transparent tunneling, see *VPN Client User Guide*, Chapter 3.

Network Interfaces

- The VPN Client cannot establish tunnels over Token Ring. However, it does not conflict with an installed Token Ring interface.
- DELL Docking Station users running the VPN Client on Windows NT may experience bluescreen failures if the latest version of Softex Docking Services has not been installed. The Softex Docking Service utilities are available directly from the DELL Support Web site, http://search.dell.com/index.asp. Select the checkbox for the File Library and search for the term “Softex Docking Services”.

Microsoft Connection Manager

Microsoft Connection Manager based dialer applications must be built with Microsoft Connection Manager Version 1.2 or greater. Include the following line in the Connection Manager section of `.cms` files used to build the dialer application:

```
DoNotCheckBindings=1
```

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.

ATT WorldNet® Dialer

Early versions of AT&T's WorldNet Dialer were incompatible with VPN services. AT&T Worldnet Setup Release 5.2.1 and higher works with VPN services. You can download the latest release of AT&T WorldNet Setup software from AT&T at the AT&T WorldNet Setup 5.2 for Windows 95, Windows 98, Windows NT 4 and Windows 2000 site at URL: http://download.att.net.

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.

Compatibility Between the VPN Client Firewall and BlackICE for Firewall Enforcement

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.

Compatibility with Visual Networks IP Insight

For the VPN Client to interoperate with Visual Networks IP Insight, you must upgrade IP Insight to Release 4.3.2.47, or higher, which has diagnostics turned off.

Compatibility with Netswitcher

All versions of the VPN Client are compatible with Netswitcher 3.1.2 and above. For the VPN Client and Netswitcher to interoperate, you must upgrade to Netswitcher 3.1.2 or higher. You can download the latest version of Netswitcher at http://www.netswitcher.com/.

Importing a Microsoft Certificate Using Windows NT SP3

The following problem has occurred on some Windows NT SP3 systems (CSCdt11315**)**.

When using the Client with digital certificates stored in the Microsoft certificate store, the Client may fail to connect. This is accompanied by the following Client event in the Log Viewer:

4101 13:41:48.557 01/05/01 Sev=Warning/2 CERT/0xA3600002
Could not load certificate (null) from the store.

Workaround: Two workarounds exist. Choose one of the following:

- Import the certificate from the Microsoft certificate store into the Cisco certificate store using the Cisco Certificate Manager. Refer to “Importing a certificate” in the *VPN Client User Guide*, Chapter 6.
- Alternatively, upgrade to a Windows Service Pack later than SP3.

Cannot Simultaneously Run the Cisco VPN Client and Windows 2000 Client

When switching between the Cisco VPN Client and the Windows 2000 L2TP/IPSec client, follow these steps (CSCdt84026):

Step 1 Stop the Cisco VPN service and disable it.

Step 2 Enable the MS IPSEC service.

Step 3 Reboot.

Log in as Administrator to Install the VPN Client

In Windows 2000, if you are logged on as User (not an Administrator) and you try to install an application, a dialog box pops up with the title that says, “Install Program as Other User”. This allows the user to login as Admin for the installation of the program *only*! Attempting to install the VPN Client using this method fails. We recommend that when you boot the system, you log in as the Administrator to successfully install the VPN Client (CSCds86139).

A problem can occur after installing the VPN Client on a Windows 2000 PC (as Administrator), and rebooting. If the first user who logs on to the PC is a restricted user, a dialog box appears advising the user that installation will not function correctly if the user is not Administrator (CSCdt16194).

The dialog box does not appear when the user logs in once as Administrator and then logs out.

Windows 98 Might Hang on Shutdown

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

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

“Q238096 - How to Troubleshoot Windows 98 Second Edition Shutdown Problems” (CSCdt00729).

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).

FTP Session Must Be in Passive Mode for VPN Client with Stateful Firewall (Always On)

An FTP session must be in "Passive Mode" when the VPN Client Stateful Firewall (Always On) is enabled. Many FTP programs support "Passive Mode" and will enable an FTP file transfer. A session from the Command Prompt uses "Active Mode" and will fail when Stateful Firewall (Always On) is enabled (CSCdv64044).

Adjusting the Maximum Transmission Unit (MTU) Value

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 1372. 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. 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

Usually, an MTU value of 1400 works. If it doesn't, the end user must decrease the value until the Cisco VPN Client passes data. Decrement the MaxFrameSize value by 50 or 100 until it works.

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

Connection Type	Procedure
Physical Adapters	Use the SetMTU utility supplied with the Cisco VPN Client.
Dial-up	Use the SetMTU utility supplied with the Cisco VPN Client.

Connection Type	Procedure
All Vendors	**Windows XP *only*** Set the following registry key value to 0: HKEY_LOCAL_MACHINE\SOFTWARE\DeterministicNetworks\DNE\Parameters\MTUAdjust Then add the following keys HKLM\SYSTEM\CurrentControlSet\Services\Ndiswan\Parameters\Protocols\0 - ProtocolType: REG_DWORD: 0x0800 - PPPProtocolType: REG_DWORD: 0x0021 - ProtocolMTU: REG_DWORD: we recommend 80 Hex or 128 Decimal  **Caution** Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable. If you are not familiar with editing the registry, contact WindRiver for help.
PPPoE Enternet	**Windows 9x** • On the main desktop, right click on My Network Places and go to Properties. The Network window opens. • Double-click the Network TeleSystems PPPoE Adapter. • On the Network TeleSystems window, click the Advanced tab, and then click MaxFrameSize. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.
	Windows 2000 • 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
WinPoet	**Windows 9x:** WinPoet does not provide user control over the PPPoE MTU under Windows 9x. **Windows 2000** WinPoet does not provide a user interface to control the MTU size, but you can control it by explicitly setting the following registry key: HKLM/system/currentcontrolset/control/class/<guid>/<adapternumber> adapter(000x) : Value: MaxFrameSize Value type: DWORD Data: 1400 (or less) The guid and adapter number can vary on different systems. Browse through the registry, looking for the MaxFrameSize value (CSCdu80463).  **Caution** Edit the registry only if you are comfortable doing so. Incorrect registry entries can make your PC unstable or unusable. If you are not familiar with editing the registry, contact WindRiver for help.

Connection Type	Procedure
RasPPPoE	**Windows 9x** • On the main desktop, right-click My Network Places and go to Properties. The Network window opens. • Find the PPP over Ethernet Protocol that is bound to the Network card that is in your PC, then double click on it. • In the General Tab check Override Maximum Transfer Unit. Change the value here. The value varies from case to case. The range can be from 1200 to 1400.
	Windows 2000 • 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

Data Transfer Problems Exist When Running on Windows 95a.

The VPN Client 3.0 or 3.1 may have data transfer problems if installed on a Windows 95a system. We recommend that you do not use the VPN Client on Windows 95a.

To check the version of Windows you have, open the Control Panel | System | General tab and look for the System version. Windows 95a is: 4.00.950a (CSCdt07587).

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

For the Windows 2000 Client, you cannot access MS resources unless you add the Client for MS Networks for the Dial-up adapter.

Disable Group Lock When Using SDI or NT Domain Authentication.

This feature is supported only when using Internal or RADIUS authentication. To ensure that you are using this feature properly please refer to the following URL: http://www.cisco.com/warp/customer/471/altigagroup.html

Raptor Mobile VPN Version 6.5.1 on Windows 2000 is not Compatible with the Cisco VPN Client

This incompatibility exists because DNE is not compatible with Raptor Mobile VPN version 6.5.1 on Windows 2000. The Raptor product uses an intermediate driver that cannot co-exist with DNE or the Windows 2000 DDK sample intermediate driver. We believe this to be a Raptor bug, since DNE can co-exist with other intermediate drivers.

Aladdin Runtime Environment (RTE) Issue with Windows NT and Windows 2000

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

“System Error: Connection Manager failed to respond.”

A side effect of this is that the VPN Client's service and dialer might become out of synch, and the PC might need to be restarted (CSCdv47999). To avoid this issue, use the Aladdin Runtime Environment (RTE) version 2.65.

Open Caveats

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

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.

Open Caveats, VPN Client Release 3.5.1

- CSCdt00735

  Certificate Manager:

  Entrust VPN Connector displays an MD5 and SHA1 Fingerprint verification for a File-based certificate request from VPN Client. The VPN Client currently does not display this Fingerprint in the request.

- CSCdt06772

  If the VPN 3000 Concentrator is configured to send a network list containing 200 networks to the Client, the Client service may fail.

  Workaround:

  Reduce the number of networks in the network list, restart the client PC, and reconnect.

- CSCdt07491

  The VPN Client may swap Primary and Secondary WINS received from the Concentrator. In a few cases, the VPN Client receives a Primary and a Secondary WINS server from the Concentrator but swaps them when they are

added to the IP Configuration. If this happens, it may cause browsing problems if the Secondary WINS server is not as populated as the Primary. Disconnecting and reconnecting may fix the problem.

- CSCdt07673

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

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

  Answer Yes every time this question appears. The installation then continues normally.

  A similar message appears on Windows NT 4.0. The message is:

  "Enternet could not find the (adapter). But it did locate the (adapter) through which your network server is reachable. Do you want to switch? Yes No"

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

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

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

- CSCdt07787

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

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

  Workaround:

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

- CSCdt10266

  Problems have occurred when attempting to make multiple client connections to the same Secure Gateway from behind a Nexland Cable/DSL router. The cause of these problems is Nexland's inability to replace the IKE source port on the second IKE session.

  A single connection works without problems.

- CSCdt13380

  When you connect the VPN Client to a VPN Concentrator that issues 2 DNS servers, both appear under ipconfig /all, but only one appears under the Network settings TCP/IP Properties. DNS server appears to be missing under TCP/IP Properties (Advanced button, DNS TAB). We do not know at this point whether this causes any problems.

- CSCdt13398

  During a split-tunnel VPN Client connection, the first packets that bring up a new IKE SA may be lost. You may need to reconnect or relaunch network applications that do not automatically try to reconnect on their own.

- CSCdt41308

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

  ```
  74    22:31:08.704  02/08/01  Sev=Warning/2   IPSEC/0xE370000C
  Failed to acquire a TCP control resource, the queue is empty.

  75    22:31:08.704  02/08/01  Sev=Warning/2   IPSEC/0xA370001A
  VRS processing failed, discarding packet
  ```

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

- CSCdt42661

  When using the VPN Client behind an ESP-aware NAT/Firewall, the port on the NAT/Firewall device may be closed due to the VPN Client’s keepalive implementation, called DPD (Dead Peer Detection). When a Client is idle, it does not send a keepalive until it sends data and gets no response.

See the description of "Allowing the VPN Client to Work Through ESP-Aware NAT/Firewalls" on page 8 in these Release Notes for more information. Refer to "Connection Profile Configuration Parameters" in the *VPN Client Administrator Guide* for a detailed description of creating profiles.

- CSCdt56343

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

  [main]
  TopMostDelay=2500

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

  Workaround:

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

- CSCdt85062

  The Cisco VPN Client Release 3.5.1, 3.1, or 3.0.X running on Windows NT or Windows 2000 does not work on an Ethernet segment that connects to a Concentrator through ATM.

  Packets > 1418 bytes are dropped.

  The VPN Client on Windows 9X works fine.

  Workaround:

  Setting the MTU with the SETMTU application allows you to work in this environment.

- CSCdu02071

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

- CSCdu20804

One of the following error messages might occur when using the Release 3.5.1, 3.1, or 3.0 VPN Client on Windows NT or Windows 2000 with the 'Start Before Logon' feature. After you establish the Client connection and then attempt to logon to the network, you might see one of the following errors messages:

- "A domain controller for your domain could not be contacted. You have been logged on using cached account information. Changes to your profile since you last logged on may not be available." This means that you are logged in at the desktop, and you can see network drives and browse the network.
- "The system cannot log you on now because the domain YOURDOMAIN is not available." This happens less often, but you can't log in at all.

At present, the only way to prevent these errors is to establish the VPN connection, then wait up to 1 minute before attempting the network logon.

- CSCdu22174

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

  Workaround:

  If this happens, delete your failed request and submit a new one.

  To delete the request, open the Certificate Manager. Click the Enrollment Requests tab, and highlight the failed request. Select Options and delete.

- CSCdu25495

  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 Entrust 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.

  Workaround:

  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”.

- CSCdu29239

  When using VPN Client with Start Before Logon (Windows NT and 2000) and Entrust Entelligence, the Entrust 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.

- CSCdu30079

  If the Nortel VPN Client version 2.51 is upgraded to version 2.62, the Cisco VPN Client detects and offers to uninstall the Nortel Client. After the uninstall completes, the user must manually reboot the PC. Setup does not automatically offer to do the reboot.

- CSCdu33638

  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.

  Workaround:

  Do *one* of the following:

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

- CSCdu35458

  During installation, the VPN Client adds a line in the registry GinaDLL=CSgina.dll. Adding this line removes the Windows XP “Welcome” screen, and you lose the ability to “switch” users. The VPN Client needs the CSgina.dll for its “Start Before Logon” feature. When the VPN Client is uninstalled, the “Welcome” screen and swap user ability are restored because the CSgina.dll is removed.

Microsoft has indicated that the “Welcome” screen and the “switch user” UI are automatically disabled in the presence of another GINA or when the Windows XP PC joins a Domain. This occurs if the registry contains GinaDLL=MSgina.dll, which is Microsoft's own Gina. Microsoft has indicated that there is nothing we can do to change this functionality. Therefore, users who want to use the “Start before Logon” feature of the VPN Client must do without the XP Welcome screen and “switch user” feature of Windows XP.

Workarounds:

– If you are *not* using the “Start before Logon” feature, you can perform the following steps to restore the Welcome screen and Switch User capability:

Caution Only edit the registry if you are comfortable doing so. Making an editing mistake in the registry can make your PC unreliable or unusable.

Step 1 Run Regedit (from the Start menu, choose Run. Type REGEDIT and click OK)

Step 2 In the left pane, click once on “My Computer” so you are at the topmost level of the registry

Step 3 Go to the Edit menu and select Find. Type in GinaDLL (case specific) and click Find Next. It should find the following registry key:

`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon` with the following value under it:

```
Name      Type     Data
-------   ------   --------
GinaDLL   REG_SZ   csgina.dll   <- the Cisco VPN Client adds this.
```

Step 4 Delete the entire value “GinaDLL”. (IMPORTANT! Do not delete the entire key called Winlogon!) Windows XP does *not* contain a default GinaDLL value.

Step 5 Exit from the registry and reboot the computer. Upon reboot, you should see the Welcome screen, and after logging in, you should see the Switch User feature.

– If you do want to use the “Start before Logon” feature, the “Start before Logon” feature uses “fall-back mode”. While this is not as elegant as when the VPN Client's csgina.DLL is installed, it does work (with some restrictions). To use “fall-back mode, you must also change the following entry in the registry:

```
\HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems\VPN Client\
Name            Type         Data
--------        ---------    --------
GinaInstalled   REG_DWORD    0x00000001   <-change to
0x00000000
```

- CSCdu42384

  The VPN Client installed on a system that was upgraded to Windows XP might not be able to establish a VPN connection using Dial-Up Networking (RAS). The symptom is that the VPN Client starts connecting, prompts for username and password, but then never finishes the connection. This problem was seen only with XP Personal/Home Edition, but it may also occur on systems that were upgraded to XP Professional.

  Windows XP systems that are 'fresh' installs do not seem to have this problem.

- CSCdu50445

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

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

- CSCdu54218

  On Windows XP and Windows 2000, at the end of the VPN Client installation, a popup box might appear in the system tray that says:

  “Local Area Connection is unavailable”

  This occurs because during the installation, networking is unavailable for a brief period while the VPN Client drivers are installed.

- CSCdu57239

  When Outlook Express is set to Work Offline mode, if you attempt to synchronize any folder with your home Exchange server, synchronization fails on any folder that has changes.

  It is successful on any folder that is already synchronized. Outlook reports a generic Network Error for each folder that fails.

- CSCdu57246

  A mechanism is needed to allow removal of a pre-defined IncompatibleGina.

  Currently, no method exists to remove a GINA from the predefined IncompatibleGinas list that ships with a VPN Client, even though the vendor has fixed the GINA and the customer now wants to use it in non-FallBack mode with the Client. No workaround currently exists.

- CSCdu61922

  If ZoneAlarm is uninstalled on a Windows 98, Windows ME, Windows NT 4 or Windows 2000 PC, then reinstalled, after rebooting the PC and launching the VPN Client, the following message might appear:

  “The VPN subsystem is not available. A connection to the concentrator will not be possible.”

  Click OK, then click Connect on the VPN Client; the connection continues normally.

- CSCdu61926

  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.

- CSCdu62212

  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 NT or Windows 2000. The first time the VPN Client dialer and service access the Entrust certificates, it prompts for a security check. This prompt displays in Windows, but not at the logon screen.

Workaround:

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.

- CSCdu62275

  VPN Client and Entrust Entelligence - VPN Connection Manager timeout.

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

Step 1 In the VPN dialer, the user clicks Connect.

Step 2 Entrust prompts for password and security hash check. The user clicks Yes.

Step 3 Entrust prompts for password for cvpnd.exe security access.

If the user waits here or walks away from PC, the Connection Manager times out in 3 minutes.

Step 4 The user returns and enters the Entrust password, then clicks Yes to the security hash check question.

Step 5 The VPN connection completes, and data can be passed. The VPN dialer appears as not connected.

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

The VPN connection can be used as a normal connection.

- CSCdu70660

  This issue occurs on an NT PC that is running ZoneAlarm, if the VPN Client is set to start before logon and an upgrade to the VPN Client is implemented. Do not attempt a connection before the logon when you reboot, because ZoneAlarm does not automatically give the VPN Client permission to access the Internet. ZoneAlarm sees the upgrade as a new application attempting to access the Internet, and it requires user permission through its pop-up menus. The user must logon to the Windows NT PC using cached credentials, then

launch a VPN connection. ZoneAlarm then asks permission to allow the VPN Client to connect. Answer yes to each connection. After that, start before logon works fine.

- CSCdu77405

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

  Workaround:

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

- CSCdu80463

  Transferring large files fails when using a VPN Client connection over a DSL/PPPoE connection. For example, if you use FTP to try to PUT a large file, it stalls and never completes. FTP GETs seem to be OK.

  This problem has been seen on Win 2000 using the Verizon DSL software (WinPoET) and Windows XP RC1 using the native PPPoE adapter. There have also been reports that this problem also occurs with NTS Enternet PPPoE software.

  Workaround:

  For WindRiver WinPoET and NTS Enternet, the following workaround is available.

  – *For systems other than Windows XP*, modify the MTU on the PPPoE adapter by explicitly changing or creating the following registry key:

    ```
    HKLM/system/currentcontrolset/control/class/<guid>/<adapternumber>

    adapter( 000x) :

             Value: MaxFrameSize

             Value type: DWORD

             Data: 1400
    ```
    (or less - you may need to experiment)

– *Windows XP* appears to work with all PPPoE software vendors. Changing the following registry keys fixes MTU related issues.

```
HKEY_LOCAL_MACHINE\SOFTWARE\DeterministicNetworks\DNE\Parame
ters\MTUAdjust to 0
```

Then add the following keys

```
HKLM\SYSTEM\CurrentControlSet\Services\Ndiswan\Parameters\Pr
otocols\0
```

```
- ProtocolType: REG_DWORD: 0x0800
```

```
- PPPProtocolType: REG_DWORD: 0x0021
```

```
- ProtocolMTU: REG_DWORD: we recommend 80 Hex or 128 Decimal
```

Caution If you are not familiar with editing the registry, please contact WindRiver or NTS for help.

- CSCdu81905

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

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

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

- CSCdu83054

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

- CSCdu84038

  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.

  Workaround:

  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.

- CSCdu86399

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

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

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

  Linksys BEFSRxx v1.39 or v1.40.1

  SMC 7004BR Barricade R1.93e

  Nexland Pro400 V1 Rel 3M

  NetGear RT314 V3.24(CA.0)

  Asante FR3004 V2.15 or later

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

- CSCdu87521

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

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

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

- CSCdv11350

  If you install a new Network Interface Card (NIC) on Windows 2000 or XP after the VPN Client is installed, the VPN Client starts to connect and complete user authentication, but it then appears stuck at “Securing Communications Channel...”. When this happens, these events appear in the Event Log:

  35 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xE300006D
  Cannot match Policy Entry:
  local host=IP ADDR=0.0.0.0, lcl_port = 0
  remote host=IP ADDR=0.0.0.0, dst_port = 0

  36 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xA3000001
  Failed to initiate negotiation.

  37 13:35:02.549 08/17/01 Sev=Warning/3 IKE/0xE3000002
  Function initialize_qm failed with an error code of 0x00000000 (INITIATE:825)

  Workaround:

  Do *one* of the following:

  – Open the Control Panel | Networking and select “Properties” for your new NIC and click OK *without* making any modifications. A rebind takes place, and the VPN Client DN driver rebinds into the IP stack for that adapter. This should work for Windows XP and 2000.

  – If that doesn't work, uninstall the VPN Client and reinstall it with the NIC card you want to use already in the PC.

- CSCdv40009

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

- CSCdv40950

  If the Stateful Firewall (Always On) is enabled but not enumerated, there is no message given to indicate that the firewall is not functioning properly.

- CSCdv42414

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

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

  Workaround:

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

- CSCdv44529

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

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

  Workaround:

  Do *one* of the following:

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

  or

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

- CSCdv46591

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

- CSCdv46937

  Using the Aladdin "R2" model etoken, certain functions can be performed using the certificate even after the R2 token has been detached from the system (USB port). The VPN Client, for instance, can perform an IKE rekey

without the token attached to the system. The reason for this is the design of the "R2" etoken: it does not contain the RSA key functions needed and must upload the private key to the system for these functions.

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

- CSCdv62613

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

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

  Workaround:

  If possible, do not use the "Allow IPSec over UDP" (transparent tunneling) feature when you have multiple VPN Client connections behind Linksys Cable/DSL router.

- CSCdv65165

  The VPN Client on Windows NT or Windows 2000 WINS servers may not be removed if the PC is shut down without disconnecting the VPN Client and the "Disconnect VPN connection when logging off" feature is disabled.

  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.

  Workaround:

  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 the correct ones for your network.

  - Alternatively, enable “Disconnect VPN connection when logging off”. Go to Options > Windows Logon Properties, check Disconnect VPN connection when logging off.

- CSCdv67594

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

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

  To do this, right-click on the Outlook icon, go to Properties, and configure it to use Microsoft Exchange or Internet Mail.

- CSCdv70215

  The following error occurs in the VPN Client log when using a Digital Certificate from the Microsoft Certificate Store. This can occur on Windows NT 4.0 with Service Pack 5 and 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”.

  Workaround:

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

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

- CSCdv76902

  If a session is already active when the Cisco Integrated Client firewall is enabled (either on the VPN Client or by policy pushed down from the Concentrator (CPP), that session is permitted to continue sending outbound packets, as long as they are not blocked by an outbound rule.

However, if the first packet sent after the firewall is enabled is inbound, the firewall does not allow the packet.

- CSCdv77711

  On a Windows 95 PC the following error may occur during a connection:

  CVPND caused an invalid page fault in module <unknown> at 0000:0400225b

  If this message appears, reboot the computer and the VPN Client will connect to the Concentrator with no problem.

- CSCdv81538

  If BlackICE Defender version 2.9 is on Windows XP and the VPN Client is reinstalled, the computer may display a blue screen (failure) upon reboot. NetworkICE and DNE are researching this issue.

- CSCdv85740

  Using BlackICE Defender version 2.9 with Windows 95 might cause a reboot or a blue screen after the connection to the Concentrator has been active for a period of time. We are working with NetworkICE to resolve this issue.

- CSCdv86736

  The following event appears in the VPN Client log upon a normal disconnect. This Event is a normal occurrence during a disconnect and was added for version 3.5 for compatibility and connection issues with Cisco IOS routers.

  57 15:22:21.016 11/12/01 Sev=Warning/2 IKE/0xA3000061

  Attempted incoming connection from 200.70.50.250. Inbound connections are not allowed.

  This happens because upon disconnect, the VPN Client sends a delete message to the VPN 3000 Concentrator and then considers the disconnect complete. When the VPN 3000 receives the delete message, it sends its own delete message to the Client. Since the Client has already completed its disconnect, the delete message from the Concentrator cannot be decrypted (because there's no connection), so this Event is displayed.

  You also see this Event if another IPSec device or Client attempts to connect to your VPN Client. The VPN Client can only initiate connections, it cannot start a VPN connection initiated from another device.

- CSCdw60866

  Getting Entrust certificates using SCEP does not get the Root CA certificate.

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

"Get certificate validity failed"
"System Error: Unable to perform validation of certificate <certificate_name>."

Resolved Caveats, VPN Client Release 3.5.1

- CSCdt52070

  The authentication on rekey applies only to VPN Client connections. You can configure this option for LAN to LAN connections, but it does not do anything.

- CSCdu04403

  VPN Client Release 3.0 installations using the oem.ini feature SilentMode are not completely Silent if there is a version of the VPN Client or VPN3000 Client already installed.

  If there is a Client already installed, you are prompted to uninstall this version. If the version being uninstalled is less than 3.0, then you are also prompted to convert the connection entry profiles before uninstalling.

- CSCdu31431

  Subnet mask in the Access-control List does not move along with the IP address when the ACL is moved up or moved down.

- CSCdu57244

  When a VPN Client has a VPN connection to the VPN Concentrator made with Dial-up Networking or with PPPoE, and you use the VPN Client to disconnect from the VPN Concentrator, the following disconnect scenario occurs.

  When the VPN Client disconnects from the VPN Concentrator, the Dial-up or PPPoE connection to the Internet remains active. You are not prompted with an option to disconnect, and you must disconnect from the Internet in the usual manner.

To disconnect from the Internet and from the VPN Concentrator in one step, disconnect from the Internet by closing the Dial-up or PPPoE connection. The VPN Client does not currently support third-party dialer disconnections.

- CSCdu64128

  When you are using Windows 2000 desktop and AOL 6.0, start before logon doesn't work. When AOL is in step 4, the VPN Client tries to connect to the Concentrator and receives the message: “Failed to connect security gateway.”

- CSCdu86637

  Using VPN Client with Entrust 5.1 SP3 or later. When disconnecting the VPN Client, it will attempt to take Entrust offline. During this time the VPN Client’s tray icon will appear with an “x” through it in the system tray for approximately 15-45 seconds. To relaunch the VPN Client dialer you must wait for this tray icon to disappear.

  This also happens when AOL is not connected to the AOL server. After this error, AOL goes through fine and connects to Internet, but the VPN connection is not established. No logs exist on the VPN Client as there is no connection on Client or on the Concentrator. The customer had problems with versions 3.0.2 and 3.0.3.

- CSCdv43452

  The VPN Client does not support Path MTU Discovery (PMTUD). This can cause some problems in certain environments with large packets.

- CSCdv47999

  This has been fixed by Aladdin in version 2.65 of the Runtime Environment (RTE).

  On Windows NT and 2000, the login prompt that is posted by the Aladdin etoken when connecting the VPN Client can get hidden in the background. If this happens, the VPN connection can timeout and fail with the following event.

  “System Error: Connection Manager failed to respond.”

  A side effect of this is that the VPN Client’s service and dialer might become out of synch, and the PC might need to be restarted.

- CSCdv71554

There is no information in the Client Systems VPN Client Connection Status tab indicating whether the Stateful Firewall (Always On) firewall is enabled. There is a note, however, indicating how to determine this status.

To verify whether the Stateful Firewall (Always On) is enabled, right-click the system tray (lock) icon. If the feature name is checked, the Stateful Firewall (Always On) feature is enabled.

- CSCdv84432

  When requesting a Certificate Revocation List, the Concentrator sends an LDAP attribute type of certificateRevocationList. This action is by default and does not have to be configured in the certificates or on the CRL web page.

  However there are some LDAP servers that require the attribute qualifier, binary (certificateRevocationList;binary). In these situations, the CRL search request fails.

  Regardless of the distribution of the ;binary qualifier the concentrator expects the CRL to be in the binary format.

- CSCdv85725

  When using Challenge based Authentication such as New PIN mode for SDI, the Command Line Interface does not present the question or reply text. The workaround is to use the HTML interface.

- CSCdw02254

  You can't configure Timeout and Retries when adding an Accounting Server via the Command Line Interface. The only things it asks for are the server name/IP address, secret, and port. To workaround this, you must modify the server and then you can change the Timeout and Retry values. You can also change the values in the HTML interface on *both* the Add and Modify actions.

- CSCdw09871

  Trying to run the VPN Client returns the following error.

  “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPSec server.”

  This may be due to a problem during the installation of the VPN Client where is exited prematurely without error. As a result some of the necessary VPN Client services/drivers do not get started after rebooting.

  To see if you have this problem, perform the following steps:

Step 1 Uninstall the VPN Client, restart the PC.

Step 2 Look in the Startup group for the following shortcut:

c:\Documents and Setting\All users\Start Menu\Programs\Startup\Cisco Systems VPN Client.lnk

Step 3 If the link exists, delete it and reinstall the VPN Client. Reinstalling should now fully complete the VPN Client install and it should run properly.

- CSCdw11058

  The VPN Client (versions 3.03 to 3.1.2) are unable to send emails larger than 740KB (including any attachments) if connected via dialup when running in Windows 2000 Professional or Windows XP. Windows 98/NT works fine.

- CSCdw15867

  Start before Logon doesn't work when greyed out

  Customer has Windows 2000, with v3.1.2VPN Client software, and wants to "lock" the start before logon feature of the VPN Client configuration by using the "!" character inside the .INI file. According to the VPN Client Administrative Guide -> Preconfiguring the VPN Client for Remote Users, the use of the exclamation point preceding each setting in the .INI file "locks" that setting so that it can't be changed in the VPN Client properties.

  When the exclamation point is placed in front of "RunAtLogon" in the .INI file, it does lock the setting so it can't be changed in the properties. However, the dialer screen never comes up, even though it is checked to come up.

  If the exclamation mark is removed, then the VPN dialer screen comes up after hitting Ctl + Alt + Del.

  This is true with versions 3.0.6,3.1.1, and 3.5

- CSCdw16291

  A Windows 98 IBM laptop with a Token Ring card has performance issues when the VPN Client software is on the laptop and the laptop is connected to the local LAN. The Client is not being launched through the Token Ring interface, but it is just installed on the same laptop with a Token Ring interface. The VPN Client in this case is not launched.

Resolved Caveats, VPN Client Release 3.5

The following problems that existed in Release 3.1 are fixed or otherwise closed in Release 3.5.

- CSCdu52740

  If the Concentrator is configured to do CRL checking to the CA, attempting to connect the VPN Client using a revoked digital certificate results in the VPN Client's hanging at the "Connecting to security gateway..." prompt for approximately 5 minutes.

- CSCdu57237

  If there is a saved password for a linked DUN connection, you are still prompted to enter the password for the connection.

- CSCdu70297

  When the concentrator is configured for an unknown vendor or product, the actual value is not recorded in the IPSec log. Instead, the values are recorded as: Null.

- CSCdu84378

  If Custom Firewall is selected on the VPN 3000 Concentrator and the Product ID number is greater than 16, the wrong message appears on the VPN Client. The message, "Unable to configure the firewall software" should be, "The Client did not match any of the concentrator's firewall configurations."

- CSCdv00237

  Windows 2000 has the ability to disable the 8.3 file and folder naming convention, but a component in the VPN Client requires that the 8.3 naming convention be enabled. If it is disabled and you install the VPN Client, you see a message that says "Can't find PROGRA".

- CSCdv10357

  The previous uninstall did not remove the VPN Client cleanly. To fix this problem delete the following registry key:

  HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion Uninstall\{5624c000-b109-11d4-9db4-00e0290fcac5}

  Then install the VPN Client.

Caution Make changes to the registry only if you are comfortable doing so. Inappropriate registry changes can cause your PC to become unstable or unusable.

- CSCdv31405

  On some IBM ThinkPad Model T22 systems with Windows XP (Build 2600) and an IBM/Intel internal NIC, you might see a Blue Screen of Death (BSOD) and random reboots when passing data during a VPN connection, or you might see the following event in the Client Event log:

  "Encrypt: Packet too large for encryption, discarding".

  This problem seems to be only with the internal mini-PCI IBM/Intel NIC in the laptop and does NOT appear to be a problem with internal mini-PCI 3COM NICs or NICs added via the PCCard slots.

  Workaround:

  Add the following entry to the registry.

  ```
  HKLM\System\CurrentControlSet\Services\TCPIP\Parameters\DisableTaskOffload = "1"
  ```

  This problem may occur on other systems that use Network Interface Cards (NICs) with DES encryption offload capabilities.

Caution Make changes to the registry only if you are comfortable doing so. Inappropriate registry changes can cause your PC to become unstable or unusable.

- CSCdv31722

  The SetMTU.exe program supplied with the VPN Client (versions 3.0.3 and 3.1) does not work with Japanese Windows 2000.

  When the dialog box pops up, there are no network interfaces available to select in the box and so the user cannot change the MTU. This problem has also been seen on French versions of Windows 2000.

- CSCdv33596

  Gemplus smart cards have a limitation that requires the certificates contained on them to have key usage of "Digital Signature" only. The version of Gemplus software tested was 3.0.30. Most commonly seen are key usages of

Data Encipherment or Digital Signature and Data Encipherment, neither of these allows the VPN Client to connect. The VPN Client Log Viewer displays the following event if the key usage is something other than Digital Signature.

259 15:36:00.209 09/14/01 Sev=Info/4 CERT/0xE3600005
Failed to RSA sign the hash for IKE phase 1 negotiation using my certificate.

Note: The key usage combination of Digital Signature and Nonrepudiation works OK.

To check the key usage of a certificate:

Step 1 Start Microsoft Internet Explorer.

Step 2 Select Tools->Internet Options->Content->Certificates

Step 3 Find the certificate in the Personal tab and click View.

Step 4 On the Details Tab, scroll down until the Key Usage option comes into view.

Step 5 Click Key Usage and view the text window below it.

- CSCdv35011

  Using digital certificates issued from a RSA Keon v5.7 CA on Gemplus smart cards does not work properly. The VPN connection fails with the following event:

  259 15:36:00.209 09/14/01 Sev=Info/4 CERT/0xE3600005
  Failed to RSA sign the hash for IKE phase 1 negotiation using my certificate.

- CSCdv38365

  If the Firewall Zone Alarm software earlier than version 2.6.357 is used on a PC with the VPN Client, Zone Alarm must be installed before the VPN Client. After installing the VPN Client, if the message, “The necessary VPN sub-system is not available...” appears, reboot the computer. The error message should not appear on the reboot.

- CSCdv43635

  Some PCs running Windows 95, Windows 98, or Windows ME have experienced problems when making a VPN Client connections using digital certificates that are large enough to require fragmentation. These problems include the PC locking up or getting an exception error with a blue screen. The issue is currently being worked on.

  No problems of this nature have been seen on Windows NT, Windows 2000, or Windows XP or while using Windows 95, Windows 98, or Windows ME and making a connection using preshared keys instead of certificates.

- CSCdv45995

  When using the CPP firewall, when the firewall tab on the connection statistics is viewed and an action (under Firewall Rules) is highlighted, using the arrow key to view the firewall statistics in the lower windows does not work.

  To view firewall policies in the lower window, highlight the specific rule in the upper window by clicking it with the mouse.

- CSCdv46713

  The VPN Client does not send the entire chain when authenticating. It sends only the ID certificate. A new configuration option will be added to allow the user to configure the device to send its entire chain except the root.

- CSCdv46726

  The error message, “The vpnclient.exe file is linked to missing export ADVAPI32.DLL Duplicate TokenEx.” may appear when using the VPN Command Line Interface (CLI) on a Windows 95B PC. This error message causes the “vpnclient.exe” command to be unusable on a Windows 95 PC.

- CSCdv49428

  Problems have occurred with some Internet firewalls where they block traffic from VPN Clients set up for IPSec over TCP on port 80. We are investigating a possible remedy for future releases.

- CSCdv57669

  On a PC with Zone Alarm (Pro) and the VPN Client, if the Client is uninstalled, on the reboot, the Zone Alarm TrueVector service may not start. If this happens, reinstall Zone Alarm (Pro) and Zone should work fine.

- CSCdv59344

  Uninstalling the VPN Client when Zone Alarm or Zone Alarm Pro version 2.6.357 is on the PC might cause the following error when the PC reboots: “Cannot find device file that may be needed...vsdata*.*”. If this error occurs, uninstall, then reinstall, the Zone Labs product.

- CSCdv63920

  When the VPN Client is connected to the VPN 3000 Concentrator and CPP rules have been pushed to the Client, if Stateful Firewall (Always On) is disabled, the event is not recorded in the ipseclog. However, the Stateful Firewall (Always On) is, in fact, off.

- CSCdv64278

  Using the VPN Client Certificate Manager application to import a certificate from the Microsoft CAPI store to the Cisco store will import all identity certificates along with the intended one. The certificates that were not meant to be imported will have to be manually deleted from the Cisco store.

- CSCdv64330

  The VPN Client cannot connect using digital certificates issued from an RSA Keon CA if the “Send CA certificate chain” option is selected. The feature defaults to disabled.

  To disable the feature, launch the VPN Client and perform the following:

  Click Options->Properties, change to the Authentication tab and uncheck the “Send CA Certificate Chain” checkbox.

- CSCdv64354

  If the Concentrator is requiring the Zone Alarm or Zone Alarm Pro firewall and the VPN Client has Zone Alarm or Pro on the PC and Stateful Firewall (Always On) is enabled, the Concentrator will report a mismatch and the connection will fail.

- CSCdv65122

  If the Concentrator does not require a Firewall and a connection is made from the VPN Client with Stateful Firewall (Always On) turned off, then during the connection Stateful Firewall (Always On) is toggled on, no data will be able to pass to the private network.

  If Stateful Firewall (Always On) is toggled on before the connection to the Concentrator, data will be able to pass to the private net.

- CSCdv70740

  If the Stateful Firewall (Always On) feature has been toggled on/off a number of times, connecting to the Concentrator might be blocked. In this state, you must reboot the PC before a connection is possible.

- CSCdv74359

  If a PC has Stateful Firewall (Always On) enabled and the PC is moved from one subnet to another, a connection to the Concentrator will not be possible unless the PC is rebooted.

- CSCdv75654

  On Windows 2000, the following BSOD occurs:

  ***STOP: 0x000000c9 (0x00000006, 0xffffffff, 0xb51fff68, 0x00000000)

  This means that the IO manager has detected a violation by a driver that is being verified. The faulty driver that is being verified must be debugged and replaced with a working version.

- CSCdv77543

  The TunnelEstablished (tunnel status) registry entry cannot be set if user is not an Administrator or Standard User and cannot be read by a Restricted or Standard User.

- CSCdv82808

  The VPN Client takes longer to connect than in previous versions. This is due to added code for the Integrated Firewall feature.

- CSCdv86885

  With Stateful Firewall (Always On) enabled, if you attempt to reconnect within approximately 2 minutes after disconnecting from the VPN Concentrator, the connection attempt might fail.

  Workaround:

  Wait 2 minutes after disconnecting, then reconnect.

- CSCdv89982

  Problems can occur when making a connection using IPSec over TCP and digital certificates over a Windows 2000 dialup connection. The failure to connect occurs only in rare cases, and then only when the VPN

Concentrator's digital certificate is of a particular size at or near the maximum MTU of 1500 bytes. The following VPN Client events appear multiple times if this is the problem, and the VPN Client fails to connect.

212 17:50:17.553 11/15/01 Sev=Info/5 IKE/0x6300002F
Received ISAKMP packet: peer = 63.67.72.132

213 17:50:17.553 11/15/01 Sev=Warning/3 IKE/0xA300005D

Unexpected message (Exchange type 6) while negotiating IKE. Message discarded.

Documentation Updates

In addition to these Release Notes, the following documents are new or have been updated for this release:

- *VPN Client User Guide for Windows*
- *VPN Client Administrator Guide*
- Online Help

Update to *VPN Client User Guide for Windows* and Online Help

In response to a customer question, please note the following clarification to the *VPN Client User Guide for Windows* and the corresponding online Help. This change occurred after the documents went to production.

In the *VPN Client User Guide for Windows*, on page 5-24, the section entitled, "Receiving Notifications from a VPN Device" should read as follows:

> The VPN device (secure gateway) through which you connect to the private network at your organization can send you notifications. Currently you can receive a notification from your network administrator when it is time to update the VPN Client software or when the VPN device that requires a specific firewall be running on the VPN Client PC detects that the firewall is not running. A notification typically shows up when you start your dialer

connection. You can also display notifications while you are connected by clicking Notifications on the Connection Status dialog box. (See Figure 5-25.)

The online Help topic for “Receiving Notifications from a VPN Device” requires the same change, except that the figure reference at the end of the paragraph is omitted.

Related Documentation

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

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

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

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/cgi-bin/front.x/case_tools/caseOpen.pl

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.

- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

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