



Release Notes for *Cisco VPN Client*, Release 3.1

CCO Date August 20, 2001



Note

You can find the most current documentation for Cisco VPN 3000 products on CCO. These electronic documents may contain updates and changes made after the hard copy documents were printed.

These release notes support VPN Client software, Release 3.1. They describe new features, limitations and restrictions, interoperability notes, caveats, and related documentation. Please read the release notes carefully prior to installation.

Contents

[Introduction, page 2](#)

[System Requirements, page 2](#)

[Installation Notes, page 4](#)

[New Features in Release 3.1, page 4](#)

[Limitations and Restrictions, page 7](#)



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

Copyright © 2001. Cisco Systems, Inc. All rights reserved.

- [Caveats, page 15](#)
- [Documentation Updates, page 39](#)
- [Related Documentation, page 39](#)
- [Obtaining Documentation, page 40](#)
- [Obtaining Technical Assistance, page 41](#)

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

Verify that your computer meets these requirements”

- Computer with a Pentium®-class processor
- One of the following operating systems:
 - Microsoft® Windows® 95 (OSR2 or greater), Windows 98, or Windows 98 second edition
 - Windows ME
 - Windows NT® (with Service Pack 3, or higher)
 - Windows 2000
 - Windows XP
- Microsoft TCP/IP installed. (Confirm by viewing Start > Settings > Control Panel > Network > Protocols or Configuration.)
- 10 MB hard disk space
- RAM (varies by operating system):
 - 16 MB for Windows 95 or Windows 98

- 32 MB for Windows NT and Windows ME
- 64 MB for Windows 2000
- 128 MB for Windows XP

**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, or
 - Network connection
 - 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

Installation Notes

Refer to the *VPN Client User Guide* for complete installation instructions.

New Features in Release 3.1

This section describes the new features in Release 3.1 of the VPN Client software.

Support for Windows XP

The VPN Client now runs on the Windows XP operating system.

Entrust Toolkit Integration

The VPN Client now supports integration with the Entrust Entelligence Client.

Client Update Notification

Release 3.1 includes the Client Update Notification feature that allows the VPN 3000 Concentrator to notify remote clients of software update options.

Local LAN Access

In Release 3.1, you can configure the VPN 3000 Concentrator to allow the VPN client access to resources on the remote user's local LAN when split-tunneling mode is not in use. The VPN 3000 Concentrator's VPN Client Local LAN option allows all users in the specified group to access all devices on their local networks. You can apply only one network list to a group, but one network list can contain up to 10 entries. You must also enable Local LAN Access on the VPN Client and on the VPN 3000 Concentrator.

For a step-by-step description of how to configure the VPN 3000 Concentrator to support VPN Client local LAN access, refer to the description of how to configure split tunneling in *VPN 3000 Series Concentrator Reference Vol I: Configuration*.

See Chapter 3 in the *VPN Client User Guide* and Chapter 1 in the *VPN Client Administrator Guide* for complete details on configuring and using the VPN Client for local LAN access.

Nortel Networks Extranet Access Client Auto-Uninstall

Release 3.1 provides the ability to automatically run the Extranet Access Client Uninstall utility and facilitate migration from the Nortel Networks Extranet Access Client to the Cisco VPN Client.

Personal Firewall Enforcement

In Release 3.1, you can configure a limited firewall policy on the VPN 3000 Concentrator. When the VPN Client connects to the VPN 3000 Concentrator on which a firewall policy is configured, a dialogue ensues that ensures that one of the firewalls running on the VPN Client matches the requirements of the VPN Concentrator.

For Release 3.1, the VPN Client provides extended support for the following firewalls (there may be other firewalls on the VPN Client system):

- ZoneAlarm Pro 2.6 (or greater)
- ZoneAlarm 2.6 (or greater)
- BlackICE Defender 2.5 (or greater) or BlackICE Agent 2.5 (or greater)

For Release 3.1, the VPN Client supports the following capability:

- Are You There (AYT)—in which the VPN Client polls the firewall every 30 seconds to determine whether the firewall is running.

For step-by-step instructions about how to set up firewall support on the VPN Client, refer to Chapter 1 of the *VPN Client Administrator Guide*. For information about configuring firewall policy on the VPN 3000 Concentrator, refer to *VPN 3000 Series Concentrator Reference Vol. I: Configuration* and the *Release Notes for Cisco VPN 3000 Series Concentrator, Release 3.1*.

Windows Logon Properties (Formerly "Start Before Logon")

In Release 3.1, the VPN Client Options menu now contains the entry Windows Logon Properties, formerly known as Start Before Logon. Three check boxes let you enable the following capabilities at the Windows Logon screen in Windows NT, Windows 2000, and Windows XP:

- Enable Start Before Logon – This is the same as in Release 3.0.
- Allow launching of third-party applications before logon – This new option can be set only by someone with Administrator privileges. It allows running of third-party applications at the logon screen.
- Disconnect the VPN Connection when logging off – If you uncheck (that is, disable) this feature, VPN Client stays connected when you log out of Windows NT, Windows 2000, or Windows XP. For more information, see the following section, "Profile Synchronization for Windows NT, Windows 2000, and Windows XP" on page 6

Profile Synchronization for Windows NT, Windows 2000, and Windows XP

You can specify whether your VPN Client automatically disconnects when you log off your Windows NT, Windows 2000, or Windows XP system. The auto-disconnect when logging off feature, which always automatically terminates your connection when you log off, is enabled by default.

Disabling this parameter allows your connection to remain up during and after log off, which allows profiles or folders to be synchronized during logoff. You would disable the auto-disconnect feature when using the Windows roaming profiles feature. If you disable the auto-disconnect when logging off feature, the VPN Client displays a warning message.



Note

With auto-disconnect disabled, you must manually disconnect or completely shut down your system to disconnect your VPN Client connection.

Limitations and Restrictions

Primary Issues in This Release

You should be aware of the following caveats regarding this release. Refer to “Open Caveats, VPN Client Release 3.1” on page 15 of these Release Notes for fuller descriptions and for the complete list of known problems.

Avoiding Extraneous Warnings When Installing the VPN Client under Windows XP

During the VPN Client installation on post-Beta 2 versions of 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 to the *.pcf (profile configuration file) for the affected connection profile. This parameter enables IKE and ESP keepalives for the connection at approximately 20 second intervals.

Use the following syntax when adding this parameter to the [Main] section of any *.pcf file:

```
ForceKeepAlives
0 - disables keepalives (default)
1 - enables keepalives
```

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

Xircom CreditCard EthernetII (CE2) Adapters

Before installing the VPN Client, verify that your Xircom adapter is running Version 3.06 or greater.

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 and Sygate Internet Connection Sharing (ICS) on Windows 98

The VPN Client is not compatible with Windows 98 Internet Connection Sharing (ICS). You cannot install the VPN Client if ICS is already installed on the same Windows 98 system. A message tells you this during installation. Do not install the Sygate ICS application after installing the VPN Client. These two programs do not work correctly on the same Windows system. For more information, see the description of “CSCdt52856” on page 35.

The Cisco VPN client can work from behind another PC running ICS by using IPsec through NAT mode.

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://support.dell.com/us/en/filelib>. Search the File Library by description for “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 5.2.1 now works with VPN services. You can download Release 5.2.1 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/rc@L50QIM631/win32dl.html>.

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.

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.

Network ICE is deciding whether future releases of BlackICE Defender will include the BICTRL.DLL file in the Network ICE distribution medium, so that you will not need to copy it from the Cisco installation release medium.

VPN Client May Disconnect with ZoneAlarm or BlackICE Defender

After making a connection from a PC with either a ZoneAlarm or a BlackICE Defender firewall, the VPN Client might disconnect with the message: "Your IPSec connection has been terminated because the required firewall software is no longer running."

Click OK and reconnect. The VPN Client will connect fine at that point.

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, 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, available at <http://www.netswitcher.com/>.

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.

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 Run the Cisco VPN Client and Windows 2000 Client at the Same Time

When switching between the Cisco VPN Client and the Win2K IPsec/L2TP client please 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).

Workaround:

The dialog box does not appear when the user logs in once as Administrator and then logs out (CSCdt36751).

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).

Other Cisco VPN Client issues

The following issues exist regarding the VPN Client:

- Rekeying and keepalives are not supported for Asante FR3004 cable/DSL routers.

When a VPN Client has an all-or-nothing connection to a VPN Concentrator through an Asante FR3004 Cable/DSL router, it can send data only over the first SA that sends data, which is usually the all-or-nothing SA. The SA to the Concentrator's public interface is blocked from sending data.

The VPN Client stays connected for a period of time in this condition, but when the two peers attempt to rekey or issue a keep-alive (DPD), the VPN Client disconnects. It appears the Asante Cable/DSL router supports only one IPSec session. This problem is even worse if the VPN Client connects using Split Tunneling. If the Networks List sent from the VPN Concentrator allows the VPN Client to access five networks, data can be sent to only one when using the FR3004.

The Asante device is supposed to support 8 IPSec sessions using 1.89 or higher code. (For more information, see - http://www.practicallynetworked.com/sharing/hwrouter_chart_pg3.htm).

We do not recommend using the Asante Cable/DSL router with the VPN Client. Our tests were done using Asante firmware 1.88 Beta and 2.02 pre-release code.

This is a problem with the Asante router, not with the VPN Client.

- 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).

- For Windows 2000 only, you must add 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.

- Do not enable the Group Lock feature 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>
- The Certificate Manager does not support export of Microsoft CAPI certificates. The GUI now tells the user it does not support this action.

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. The following lists are sorted by bug ID. Change bars in the margin indicate differences from the previous Beta release.



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/support/bugtools>.

Open Caveats, VPN Client Release 3.1

- 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.

- CSCdt07748

Issues exist when running the VPN Client Release 3.0 and ZoneAlarm version 2.1.44.

To configure ZoneAlarm version 2.1.44 to work with the VPN Client, do the following steps:

Step 1 In ZoneAlarm, click Programs.

- Step 2** Choose “Allow Connect for the Cisco Systems VPN Client” and “XAUTH Application”.
- Step 3** When starting the VPN Client on a PC that has ZoneAlarm version 2.1.44 you might see the following message:
- “The necessary VPN sub-system is not available. You will not be able to make a connection to the remote IPsec server.”
- Step 4** Click “OK”. When you retry, you will connect using the VPN Client.
-

- 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.

- CSCdt14787

When a VPN Client has a VPN connection made with Dial-up Networking or with PPPoE to the VPN Concentrator, 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.

- 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.

- CSCdt46415

If the VPN Client on Windows NT or 2000 is configured for Start before Login and has an application configured in Application Launcher, that application loads before the login occurs, but is hidden after you log in. You cannot load another instance of the same application, and trying to do so causes an error.

Workaround:

Press CTRL-ALT-DEL to get to the Windows Security screen. On that screen, you should see the application you loaded from the Application Launcher. Close the application, then click Cancel on the Windows Security screen. Now you should be able to re-run the application without errors.

- CSCdt85062

The Cisco VPN Client Release 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 GUI loads during a shutdown or restart of the operating system. This will not cause any problems and can be ignored.

- 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 appropriate “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 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 was 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 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

In a Windows XP environment, installing the VPN Client removes Welcome screen and swap user ability.

During installation, the VPN Client adds a line in the registry
GinaDLL=CSgina.dll.

When this line is added, the Windows XP “Welcome” screen is removed and you lose the ability to “swap” users. Even after uninstalling the Client, these features are not returned to their normal state. You must delete the GinaDLL line from the registry to regain this functionality.
 - 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 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, the VPN Client must be installed after Entrust SignOn because the VPN Client replaces the Entrust GINA (etabegin.dll) with its own (csgina.dll).

- 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 client hanging at the "Connecting to security gateway..." prompt for approximately 5 minutes.

- 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.

- CSCdu57237

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

- 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.

- CSCdu57240

Windows ME: Novatel Ricochet modem does not function with VPN Client
Metricom provides customers with three different connectivity options for use with the Ricochet (128K wireless WAN) service.

- Sierra Wireless Aircard 400 Ethernet (PCMCIA Ethernet Card)
- Novatel Wireless Modem (PCMCIA modem)
- Metricom RICOCHET GS Wireless Modem (USB modem)

The Novatel Wireless modem functions properly with the VPN client on Windows 2000 and Windows 98. On Windows ME, the Novatel Wireless modem can no longer pass packets of approximately 1400 bytes or longer if the VPN client is installed on the system (even if the VPN Client is not in use). Windows 95 has not yet been tested.

The Sierra Wireless Aircard has been successfully tested on Windows 2000 and Windows 98, but cannot yet be tested on Windows 95 or ME because there are no drivers for these Operating Systems available from Sierra Wireless.

Interoperability with the Metricom Richochet GS Wireless Modem has not been tested.

Workaround (for Windows ME):

-
- Step 1** On the System Control Panel, choose Network, then choose the Dial Up Adapter.
 - Step 2** Choose Properties.
 - Step 3** On the Advanced Tab, choose the IP Packet Size and change from Automatic to Medium.
-

- CSCdu57241

Domain controller could not be contacted - using Start before Logon

One of the following error messages might occur when using the Release 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” - you are 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” - happens less often but you can't login 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.

- CSCdu57244

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

- 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 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 3.1 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 this is done it can be used 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 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:

1. In the VPN dialer, the user clicks Connect.
2. Entrust prompts for password and security hash check. The user clicks Yes.
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
4. The user returns and enters the Entrust password, then clicks Yes to the security hash check question.
5. The VPN connection completes, and data can be passed. The VPN dialer appears as not connected.
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.

- 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.

- 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.

- CSCdu79874

VPN Client uninstall fails on Windows 2000 with the Verizon/WinPoET PPPoE client.

Uninstall of the VPN Client fails to complete if a PPPoE connection was made, then a VPN Client connection was established, and data was sent. This was found to occur using the Verizon DSL Client (WinPoET PPPoE client by Wind River Systems v2.0 or 3.0). If you reboot and *never* make a DSL/PPPoE connection, then the VPN Client should uninstall without a problem.

- 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 will stall and never complete. FTP GETs seem to be OK.

This problem has been seen on Windows 2000 using the Verizon DSL software (WinPoET) and Windows XP RC1 using the native PPPoE adapter.

- 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 will need to have Entrust digital certificates renewed by placing them directly on the network during the renewal period to get updated.

- 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 client. The message, “Unable to configure the firewall software” should be, “The Client did not match any of the concentrator’s firewall configurations.”

- 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, a VPN 3000 Concentrator). The problem is with the Cable/DSL router, not with the VPN Client or the Gateway.

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 may *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 Linksys BEFSR401, SMC Barricade 7004BR, D-Link DI-704 and *many* other inexpensive Cable/DSL routers on the market. We have been in contact with a few of these vendors to try to resolve the issue, but no changes have been made so far.

- CSCdu86637

VPN client and Entrust Entelligence - tray icon delay

Using VPN client with Entrust 5.1 SP3 or later, the VPN Client, when disconnecting, attempts to take Entrust offline. During this time, the VPN Client's tray icon in the system tray appears with an 'X' through it for approximately 15-45 seconds. To relaunch the VPN client dialer, you must wait for this tray icon to disappear.

- 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)
```

- CSCdu88694

If you configure Windows XP Pro RC2 to login to a Windows 2000 domain and use the Client's Start Before Login feature to connect, it might take up to 10 minutes to log in to the Windows 2000 domain. This does *not* happen when logging into a Windows NT 4.0 domain. We are looking into this issue and hope to have a solution by the time Windows XP is officially released.

- 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".

Workaround:

Ensure that the 8.3 file and folder naming convention is enabled.

Resolved Caveats, VPN Client Release 3.1

The following problems that existed in Release 3.0 are fixed or otherwise closed in this release. Change bars in the margin indicate differences from the previous Beta release.

- CSCds23081

When a VPN tunnel is established, addresses on the User's local subnet are not accessible. ARPs and DHCP requests go out on the local LAN in the clear. All other traffic for the local addresses goes out on the local subnet encrypted. However, the local LAN does not allow traffic to go through the tunnel, out onto the Internet, then back to their own LAN.

- CSCds65138

For Windows 2000 only, you must add Client for MS Networks for Dialup Connections. Otherwise, issues exist with network browsing, printing, drive mapping, etc., over dial-up networking connections.

For the Windows 2000 client, you cannot access MS resources unless you add the Client for MS Networks for the Dial-up adapter. Add and enable this during installation, as described in the following steps:

-
- | | |
|---------------|---|
| Step 1 | Open the “Network and Dial-up Connections” dialog.
From the Desktop, right-click on “My Network Places” and select “Properties”. |
| Step 2 | In the “Network and Dial-up Connections” dialog, right-click on the dial-up connection to be modified and select “Properties”. |
| Step 3 | Click the “Networking” tab and view the list of components in the listbox. |
| Step 4 | Check the “Client for Microsoft Networks” checkbox. |
| Step 5 | If the “Client for Microsoft Networks” is not there, click the “Install” button, select “Client”, and click “Add”. |
-

- CSCds70230

When the VPN Client is installed on a Windows NT or Windows 2000 system, LAN Netware Networking no longer functions.

We have reproduced this issue when the IPX Frame Type is set to anything other than 802.2. Please report Netware-related issues only if this is not your problem.

If your frame type is set to 802.3 or 802_II, Netware stops functioning with the client installed.

Workaround:

Change Netware server and client frame types to 802.2 or add another frame type to the Netware server of 802.2.

Changing the frame type on a Netware can be difficult in a multiserver environment. The frame types must be the same on all the servers for them to see each other. With NDS, the servers lose connectivity with each other, and this could cause NDS tree problems or NDS replication problems.

The easiest thing to do is to add an additional frame type on the server and bind the frame type to the interface on the Windows 2000 system.

- CSCds73159

System lockups have occurred when using the VPN Client on a machine with the RASPPPOE PPPoE Client.

- CSCdt05705

The following behavior was observed at a customer installation that has a mail server reachable from the Internet and from the inside network. When the tunnel is established, a query done with nslookup queries the outside DNS and returns the private address; a PING queries the inside DNS and returns the public address.

The behavior described is by design. The customer says that this is a bug, and that the OS should use the one DNS entry that was given to the PC by the concentrator.

No support for Dual DNS in Split tunnelling is planned. A change was made (see below) to preserve the existing DNS entries in the search list. This change appends existing DNS entries onto the Concentrators DNS list. This appended list is supported to varying degrees by the Microsoft OSs. For example Windows 95 supports only the first two entries of a search list.

When the VPN Tunnel is established the Domain Search list is overwritten with the VPN server. The code now appends the existing DNS addresses to the end of the new list.

- CSCdt06786

Windows 95 NetLogon GUI fails to pop up after tunnel connects to VPN 3000.

- CSCdt10649

Network Browsing over America On Line (AOL) version 5.0a now works correctly as long as the WINS configuration is set to use DHCP for WINS resolution and the AOL adapters are bound to “Client” for Microsoft Networks.

- CSCdt11516

Sometimes, when using the VPN Client feature “Start before Logon”, you can establish a VPN connection, login to the Domain, and the Client “lock” icon does not appear in the Windows system tray. The VPN Client is still connected at this point; it's just the icon that does not appear. To work around this issue, run the VPN Dialer from the Programs menu. The icon then appears in the system tray.

- CSCdt22364

When the Verizon WinPoet software, version 3.0 build 20000427 is installed on a Windows 2000 SP1 PC with the VPN Client, a connection can not be made to the Internet. If the Verizon software is installed before the VPN Client, you will get an error when trying to connect to the internet. If the VPN Client is installed first, the Verizon software gives the message: “Failed to detect the IVasion Adapter, verify that the IVasion Adapter is installed.”

If you uninstall the VPN Client, connections to the Internet will succeed.

When the Verizon WinPoet software, version 3.0, is installed on a Windows 2000 PC with the VPN Client, you cannot make a connection using WinPoet. If you install the VPN Client first, the WinPoet software gives the message:

“Failed to detect the IVasion Adapter, verify that the IVasion Adapter is installed.”

You can use RAS PPPoE on Windows 2000 with the VPN Client.

If you uninstall the VPN Client, WinPoet connections succeed.

- CSCdt29220

When connected to a corporate network, browsing the network through Network Neighborhood may stop working if File and Print Sharing is enabled on the VPN Client PC. If File and Print Sharing is turned off, browsing should work fine.

To disable File and Print sharing on the VPN Client, follow these steps:

-
- Step 1** Right click on the Network Neighborhood icon on the desktop.
 - Step 2** Select Properties.
 - Step 3** Click File and Print Sharing.
 - Step 4** Uncheck the “I want to be able to give others access to my files” check box.
 - Step 5** Click “OK”, then “OK” again.
 - Step 6** You might be asked for the Windows installation disk; if so, put it into the drive and click “OK”.
 - Step 7** When prompted, reboot the PC.
-

- CSCdt23222

At this time, the VPN Client is not compatible with the Microsoft Operating System code named Windows XP (formerly codenamed “Whistler”). Do not attempt to install the VPN Client on Windows XP.

- CSCdt23662

You cannot access workgroups through Network Neighborhood. When you click on a Workgroup in Network Neighborhood, the following message might appear: “Workgroup is not accessible. The computer or sharename could not be found. Make sure you typed it correctly and try again.”

- CSCdt34053

With certain types of software (including the SyGate personal firewall) installed on Windows 2000, after the VPN Client disconnects, an error appears that says “System error: Connection manager failed to respond” [OK]. The only problem this causes is that you must wait about one minute before you can connect again.

- CSCdt35159

A shortcut icon for the VPN Client added when Release 2.x was installed does not work when you install Release 3.0 or higher. The reason for this is that the two versions install to different directories, and the executable files between the versions are also different. This is normal behavior.

Workaround:

Delete the old shortcut icon and add a new one using the Release 3.1 VPN Client (Options | Create a Shortcut).

- CSCdt35199

Sometimes on Windows NT, the InstallShield Setup Status screen stalls at 100% and never continues. This screen *should* go away just before the last installation screen with the FINISH button appears, but we have seen a couple of cases where it doesn't go away.

To finish the installation, simply move the Status window to the side. You should see the last screen with the FINISH button behind it. Click FINISH, and the PC reboots. In most cases, the installation is complete. To be absolutely sure, we recommend you uninstall the client, reboot, and re-install the Client.

- CSCdt35280

The VPN Client software resumes an install after an uninstall, even though the Windows NT PC only logged out the user and did not do a complete reboot.

You may run into this situation if you are running Windows NT and there is an application that is misbehaving (that is, hogging CPU cycles). The VPN Client uninstall attempts to reboot the Windows NT PC. The PC may simply log the current user off and resume at the ctrl-alt-delete screen without actually rebooting. The client software does not prohibit the installation of the new version, even though the required boot cycle did not complete.

To rectify the situation, make sure that the PC completes a full boot before resuming the install.

If you try to do an install after doing an uninstall without first rebooting the PC, the install aborts.

- CSCdt38940

If AOL is installed on a PC that also has the VPN Client, you will not be able to dial out using the VPN Clients option - Dial-Up Networking Phonebook Entry. This option is found under the VPN Clients options/properties Connection tab. Instead, use the third-party dial-up feature found under the Client's options/properties Connection tab.

- CSCdt44264

If you use an OEM.INI file that does NOT have DefGroup=something in the [Default] section, the Client shortcut files are installed to the root of the Program Group. To place the Client shortcut icons in their own group, add DefGroup=Your Group Name in the OEM.INI file. ("Your Group Name" can be anything you want).

- CSCdt44471

Running Netmon on a Windows 2000 PC with the VPN Client installed is not recommended.

Netmon may display capture data incorrectly if other VPN Client activity is present on the network. If the VPN Client Log Viewer is running it may also incorrectly display messages while Netmon is capturing.

- CSCdt45375

The VPN Client and the personal firewall TP Firewall version 2.0.9 are not compatible on a Windows ME PC. When the VPN Client is installed after TP Firewall version 2.0.9 on Windows ME, an exception occurs on the PC and the computer displays a blue screen when booting up. Windows loads after the blue screen appears after you hit any key, but the client does not operate. The workaround is to remove TP Firewall before installing the VPN Client.

- CSCdt45403

On Windows NT and Windows 2000, you can configure the VPN Client to "Start Before Logon" and to use a third party dial-up application (not Microsoft Dial-Up Networking). When using these two features together, the third party application always appears behind the VPN Client and cannot be brought to the foreground. To resolve this, move the VPN Client window to one side before clicking Connect. This should leave plenty of room on the screen to use the third party dial-up application.

- CSCdt47367

The UDP keepalives sent from the client cause the client connection to remain active even after the ISAKMP delete has been received. Therefore, the client is never truly disconnected due to inactivity.

Each time the ISAKMP delete message is sent, the event log shows a message stating that the client has been disconnected due to idle timeout. However, within session management the connection still remains active and traffic can continue to pass.

- CSCdt52856

When disconnecting the VPN Client on a PC that has the Sygate Personal Firewall installed, you may get the following message:

System Error: Connection Manager Failed to Respond.

If you see this message, click OK. You will not be able to reconnect with the Client for a few minutes. Wait a few minutes, and the Client will be able to re-connect with no problem.

- CSCdt57056

When doing IPsecUDP (NAT), packets that are received out of order are not always properly reassembled, causing the client to display “could not find cached fragment” messages and the connection to not function.

IPsec (non UDP) does not exhibit this behavior.

- CSCdt57552

Login to Domain stalls on Win2k Client - 2000 only Network-Kerberos

This problem occurs when “Start before Logon” is used on a Windows 2000 VPN Client. After the Client is connected to the Concentrator and the user attempts to log into a Windows 2000 only Domain, the PC seems to lock up at the point where it's “Loading your personal settings...”.

This problem occurs if the user belongs to more than two Groups. If the user belongs to only one or two Groups, this problem does *not* occur. They can login to the Domain just fine and are left at the Windows desktop.

- CSCdt59801

If the client is uninstalled or upgraded (which does an Uninstall) from a mapped network drive, it receives an error as soon as you click OK after being prompted to reboot:

“Program Error: setup.exe has generated errors and will be closed by Windows. You will need to close the program. An error log has been created.”

You must go to the Task Manager and stop the Install Shield application. After doing this, you receive an ikernel.exe “program not responding error.”

There appears to be no negative impact other than this annoyance. To avoid this message, do not install the VPN Client from a mapped network drive.

- CSCdt63783

An “Application Error” in CVPND.EXE on NT or “Invalid page fault in CVPND.EXE” on Win9x might occur if you enter an incorrect username or password when the Client rekeys IKE. The Client reprompts for authentication information on rekey only if you have Reauthenticate on Rekey enabled on the Group in the Concentrator.

- CSCdt71503

The Application Launcher cannot properly launch CRYPTOCARD ST-1 software tokens.

CryptoCard has provided two files to help solve this problem. ST1.EXE and an ST1.ini can be used instead of trying to run the Java application. This works with the Application Launcher and can be obtained from CryptoCard; or it also ships with CryptoAdmin 5.1.

- CSCdu53939

With Windows XP, a hardware installation warning appears during Deterministic Networks install-Miniport

During the VPN Client install on Windows XP builds after Windows XP Beta version 2, an error message might appear that says:

“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.

If you are installing under Windows XP, *before you install the VPN Client*, go to Start | Control Panel | System | Hardware | Driver Signing and set Windows XP Driver Signing to Ignore. This avoids these messages

- CSCdu56588

On Windows 98 SE, Windows ME, and Windows NT 4.0 SP 6, if the VPN Client is installed before the firewall ZoneAlarm Pro, the VPN Client does not detect ZoneAlarm until the PC is rebooted. Because ZoneAlarm Pro does not require a reboot after being installed on the listed operating systems, you must manually reboot.

- CSCdu61306

On a Windows NT 4.0 PC, a Dr Watson error in IPsec dialer might appear if the VPN Client is set to start before logon and the firewall ZoneAlarm is installed in the PC.

- CSCdu63965

This functionality conforms to the feature design and is documented in the manual.

When the VPN Client is connected and configured for local LAN access, you cannot print or browse by name on the local LAN. When the VPN Client is disconnected, you can print or browse by name.

You can browse by IP Address or to print, you can change the properties for the network printer to use the IP Address instead of names. For example instead of the syntax `\\sharename\printername`, use `\\x.x.x.x\printername`, where x.x.x.x is an IP address.

To print and browse by name, you can use an LMHOSTS file. To do this, add the IP addresses and local hostnames to a text file named LMHOSTS and place it on all your local PCs in the \Windows directory. The PC's TCP/IP stack then uses the IP address to hostname mapping in the LMHOSTS file to resolve the name when printing or browsing. This approach requires that all local hosts have a static IP address; or if you are using DHCP, you must configure local hosts to always get the same IP address.

Example LMHOSTS file:

```
192.168.1.100 MKPC
192.168.1.101 SBPC
192.168.1.101 LHPC
```

- CSCdu65330

Sometimes an error appears just after you login to Windows 2000 or NT, and when you click OK, the VPN Client main GUI window may appear. The error says:

“Cisco Systems VPN Client

=====

Connection entry “run_only_if_connected” does not exist.”

This error is very minor and it will be fixed after the initial 3.1 Beta release.

- CSCdu68581

After making a connection from a PC with either ZoneAlarm or BlackICE Defender, the VPN Client might disconnect and the following message will appear: “your IPSec connection has been terminated because the required firewall software is no longer running.”

Click the OK button and reconnect. The VPN Client will connect fine at that point.

- CSCdu70340

During a connection to a Concentrator requiring ZoneAlarm, if the ZoneAlarm TrueVector service is shut down on a Windows NT 4.0 SP 6 PC running ZoneAlarm, the tunnel is terminated. If you attempt to re-establish the tunnel, the following Dr Watson error may occur:

```
CVPND.EXE
Exception: access violation (0x00000005), Address:
0x004cc288
```

We strongly recommend that you do *not* stop the firewall service during a connection.

- CSCdu79818

When the v3.1 VPN Client is installed, the following registry entry is added:

```
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\YourApp.exe
```

If you install v3.0, this key is added instead:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\ipsecdialer.exe

A mistake was made in the v3.1 InstallShield script and it will be fixed in the final v3.1 release. The correct entry in the registry should be:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App
Paths\ipsecdialer.exe

- CSCdu80585

When Start Before Logon is enabled on a Windows NT 4.0 SP 6 PC, the VPN Client might appear to lock because nothing happens when the user clicks on the connect button. The PC is not locked at this point. Wait for up to 30 seconds and the Authentication for... dialog box appears and the password can be entered normally. The connection will continue at point.

Documentation Updates

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

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

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/tac/caseopen>

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.

AccessPath, AtmDirector, Browse with Me, CCDA, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco Powered Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Discover All That’s Possible, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Voice LAN, Wavelength Router, WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site 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. (0101R)

Copyright © 2001, Cisco Systems, Inc.
All rights reserved.

