Release Notes for the Cisco VPN Client, Release 3.7.3 for Linux, Solaris, and Mac OS X

CCO Date: February 7, 2003

Part Number: 78-15475-01

Note You can find the most current documentation for the VPN Client at http://www.cisco.com or http://cco.cisco.com. These electronic documents may contain updates and changes made after the hard copy documents were printed.

These Release Notes support VPN Client software Release 3.7 for the Linux, Solaris, and Mac OS X operating systems and for the incremental "point" releases: Release 3.7.3.A, Release 3.7.3 and Release 3.7.2. Please note that there is no Release 3.7.1. These release notes are updated as needed to describe new features, product and procedure changes, caveats, and related documentation. Please read the release notes carefully prior to installation.

This document contains a new section, "Usage Notes," describing interoperability issues. In addition, the caveats lists are reorganized to conform with the other Cisco VPN product Release Notes, so that open caveats come first. Resolved Caveats are grouped according to the release that contains the fix. Within a release, caveats are now listed in ascending alphanumeric order, rather than by operating system, because some caveats apply across platforms.

Contents

This document contains the following sections:

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

New Features

Releases 3.7.3 contains one new feature, as well as a number of fixes to caveats from previous releases. Release 3.7.2 fixes a number of caveats that were outstanding in Release 3.7, but does not introduce any new features.

New Feature in Release 3.7.3

Release 3.7.3 offers the following enhancement to the VPN Client:

The VPN Client now preserves the original “search...” settings in /etc/resolv.conf file when connection is made and new DNS-related parameters are received from VPN 3000 Series Concentrator. This is especially important if a host uses =several= domains originally listed in the “search...” string (CSCdz80277).

New Features in Release 3.7

The features in the following list were introduced in Release 3.7.

- Release 3.7 adds a graphical user interface for managing the VPN Client for Mac OS X, in addition to the command-line interface. Refer to the *Cisco VPN Client User Guide for Mac OS, Release 3.7* for more information.
- The installer for the VPN Client for Solaris is now packaged as a single installation file for all supported Sun platforms.
- The VPN Client for Linux now supports ISDN connections in addition to PPP and Ethernet.
- The VPN Client on the Sun Solaris platform now supports PPPoE, PPP Version 4.0, and Solaris Version 9.

System Requirements

The VPN Client supports:

- Red Hat Version 6.2 or later Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.

Note The VPN Client for Linux does not support kernel Version 2.5 or SMP (multiprocessor) kernels.

- UltraSPARC computer running a 32-bit or 64-bit Solaris kernel OS Version 2.6 or later.
- Macintosh computer running OS X Version 10.1.0 or later.

Supported Hardware

The Cisco VPN Client supports the following Cisco VPN devices:

- Cisco IOS software devices that support Easy VPN server functionality
- VPN 3000 series concentrators
- Cisco PIX Firewall series, Version 6.2 or later

Usage Notes

Usage notes describe interoperability issues and known behavior of the VPN Client. These are not caveats (although a caveat identifier may appear in parentheses after a description). Rather, these are things that may not be obvious to users or that occur only in special circumstances.

VPN Client on Solaris Platforms Does Not Support the ipdptp Dialup Interface

The VPN Client Releases 3.7.2 and higher no longer support the ipdptp dialup interface on Solaris platforms. This ipdptp interface is used for dialup connections on the Solaris 6, 7, and 8 platforms. Solaris 8 users can obtain a standard patch from SUN. This patch lets you use the new pppd 4.0 driver, which is still supported by the VPN Client. Newer Solaris 8 installations and Solaris 9 use pppd 4.0 as their standard dialup and PPoE driver.

- Solaris 6 and 7 users who want to keep the ipdptp dialup interface must remain with the VPN Client, Release 3.7.1 or earlier.
- Solaris 8 users may apply the patch that will allow them to use the new pppd 4.0 driver from SUN (CSCdz48205).

Switching Interfaces While Connected Is Not Seamless

When using the VPN Client connection while roaming over wireless, if the workstation is then connected over Ethernet, the VPN Client connection no longer passes traffic until a new connection is established.

The VPN Client does not sustain a VPN Client tunnel when an interface or IP address changes after it made its initial connection. This might also happen when roaming between wireless stations that change the IP address of the workstation as it moves through zones.

This is just the behavior of the VPN Client when switching interfaces and IP addresses, which is usually done while roaming wireless.

You must disconnect the VPN Client before switching interfaces or IP addresses (CSCdz81761).

VPN Client on Non-Windows Platform Does Not Support Multiport Adapters

The Solaris, Linux, and Mac OS X VPN Clients do not support multiport adapters such as dual and quad FastEthernet (CSCea78807).

Open Caveats for Release 3.7.3

- CSCdv54087

  When connected over a PPP connection using any of the Linux, Solaris, or Mac VPN Clients, the Excluded networks do not allow traffic to the network directly connected to the workstations ethernet adapters.

  The EnableLocalLan keyword combined with the proper Concentrator Group configuration should allow the VPN Client to pass traffic to the workstations local Ethernet network. An issue with the client prevents traffic only to the network directly attached to the workstation. Other networks excluded from the tunnel pass traffic normally.

  Workaround:

  An alternative to excluding networks is to create a list of only those networks to be tunneled. This could be configured on the Concentrator and would allow access to the directly connected network to the workstation.

- CSCdv73541

  The make module process fails during installation of the VPN Client.

  Workaround:

  The module build process must use the same configuration information as your running kernel.

  – If you are running the kernels from Redhat, you must install the corresponding kernel-sources rpm. On a Redhat system with kernel-sources installed, there is a symlink from /lib/modules/2.4.2-2/build to the source directory. The VPN Client looks for this link first, and it appears as the default value at the kernel source prompt.

  – If you are running your own kernel, you must use the build tree from the running kernel to build the VPN Client. Merely unpacking the source code for the version of the kernel you are running is insufficient.

- CSCdw27781

  If an IP firewall is installed on your workstation, the reboot after installation of the VPN Client takes an inordinate amount of time. This is caused by a conflict between the VPN Client kernel module cipsec and the ipfilter firewall kernel module.

  Workaround:

  Disable the ipfilter firewall kernel module *before* you install the VPN Client.

- CSCdw60694

  The VPN Client does not function if it is installed on a Linux system using hotplug.

- CSCdy16607

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

On a PC with ZoneAlarm Plus version 3.1.274 and the VPN Client, the following error occurs when the PC boots:

On Windows 2000:

> ZAPLUS.exe has generated errors and will be closed by Windows. You will need to restart the program.
>
> An error log is being generated.

The Application Log states:

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

Similar errors occur on other Windows operating systems.

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

Workaround:

Use ZoneAlarm v.2.6.362 or ZoneAlarm Pro v.3.0.133.

- CSCdy30098

  If you use the VPN Client for Solaris with the pppd Version 4.0 driver over PPPoE, the client can establish a VPN connection, but cannot pass traffic. This occurs because the client is unable to pass traffic if used with a PPPoE connection exclusively. The VPN Client must first attempt an hme connection, even a failed one, to properly prepare for the PPPoE connection.

  Workaround:

  a. Restart the Solaris workstation.

  b. Attempt a VPN connection while the PPPoE link is down. You might be required to assign a false address to the hme interface if it does not have one. It is not necessary for this connection attempt to succeed.

  c. When the connection times out, restore the PPPoE connection.

  VPN traffic should pass normally. If you restart your workstation for any reason, you must repeat this process.

- CSCdz01693

  The VPN Client does not provide a 30-day warning when your certificate is near expiration or when your user identity certificate is near expiration. If your certificate expires, the following message appears:

  > Unable to contact security gateway.

  Workaround:

  Confirm your expiration date on the Certificates tab in the Validity field.

- CSCdz02799

  If you launch the VPN Client for Mac OS X GUI from a terminal, you might see messages like the following on the terminal:

  Oct 10 13:05:24 Rhsturm /Applications/VPNClient.app/Contents/MacOS/VPNClient:

  *** Warning: Line option kATSLineIsDisplayOnly has been deprecated. ***

  Oct 10 13:05:24 Rhsturm /Applications/VPNClient.app/Contents/MacOS/VPNClient:

  *** Warning: ATSUMeasureText has been deprecated. Use ATSUGetUnjustifiedBounds instead. ***

Workaround:

Launch the VPN Client from the Finder, or from the Dock or Desktop icon.

- CSCdz04238

  The progress bar for the VPN Client for Mac OS X installer does not accurately reflect the progress of the installation process, which takes an inordinate amount of time.

- CSCdz58821

  Using the VPN Client over a SuSe native PPPoE connection, the VPN Client

  fails to connect. The VPN Client cannot bind to the type of PPPoE used natively by SuSe.

  Workaround:

  Download and install the Roaring Penguin version of PPPoE, which has been tested successfully with the VPN Client.

- CSCdz77884

  On a Linux system, the VPN Client version 3.6.3, 3.7, and 3.7.2 fail to obtain a certificate from an RSA KEON CA server version 6.0.2 or version 6.5 build 148.

  The VPN Client shows the following message on screen after going through the enrollment procedures:

  ```
  contacting certificate authority.
  error: certificate enrollment failed.
  ```

  The event log debugs for this attempt show the following:

  ```
  1      11:57:32.585  01/13/2003  Sev=Info/5 CERT/0x43600001
  Success: enveloped message.

  2      11:57:32.683  01/13/2003  Sev=Info/5 CERT/0x43600001
  Success: signed message.


  3      11:57:32.683  01/13/2003  Sev=Info/5 CERT/0x43600001
  Success: Encrypted and Signed PKCS request message.

  4      11:57:33.004  01/13/2003  Sev=Warning/2 CERT/0xC3600016
  Failure on: CEP response VERIFY.
  ```

  Windows VPN Clients can obtain certificates from the same RSA KEON CA server successfully without issues.

  Workaround:

  Don't use certificates for the Linux VPN Client connections from an RSA KEON CA server version 6.0.2 or version 6.5 build 148. Use pre-shared keys.

- CSCdz78215

  While attempting to make a VPN Client connection from a Linux system, the workstation crashes if PPPoE is activated during the connection. If a VPN Client connection is in progress while PPPoE is being brought up, the workstation also crashes.

  Workaround:

  Disconnect the VPN Clientconnection attempt before activating PPPoE.

- CSCdz79762

Some Classic Mac applications might have problems sending/recieving large packets over the VPN when using the Release 3.7.2 VPN Client GUI on MacOS X 10.2

Workaround:

Third-party applications such as OT Advanced Tuner can manually set the classic environment MTU/MSS settings. Setting the MTU/MSS setting to 1300 should remedy this behavior.

The MacOS X classic environment seems to have stopped inheriting its MTU settings from the MacOS X network stack, somewhere in the 10.2 releases. It's possible that it never inherited these settings, and we merely never saw the problem before, because most Classic Mac applications use pMTUdiscovery to adjust MTU/MSS settings. We only alter the MTU settings of the MacOS X network stack.

- CSCdz88631

  When installing the VPN Client on a Red Hat 8.1 beta installation, a number of disquieting warnings appear during installation as well as a strange binary message while connecting the VPN Client. Although inimical, these messages do not affect the performance of the VPN Client.

Caveats Resolved in Release 3.7.3

This section lists the caveats resolved in the Cisco VPN Client Release 3.7.3.

- CSCdx33045

  A Linux workstation becomes inoperable when you use the VPN Client with a PPP connection and configured to use SecurID for authentication. This occurs using kernel revision 2.4.7 to 2.4.17 on Red Hat.

- CSCdy62416

  The VPN Client does not establish a connection using a digital certificate to the central-site Concentrator when behind a NAT device that prevents or corrupts IP fragments.

- CSCdy66378

  On some laptops, when using an onboard Ethernet card, the DNS server information that is pushed down through mode config is not used. Using a PCMCIA adapter on the same laptop works fine.

- CSCdy81064

  When the adapter address changes, we disconnect the VPN Connection, but the only message in the logs states:

  ```
  111    13:58:38.601  10/03/02  Sev=Info/4CM/0x6310001F
  Adapter address changed. Terminate secure connections
  ```

  We should have better log messages to debug this problem.

  The old message was removed, and the following two new messages were added.

  When the connection is established, we display the log message:

  ```
  Address watch added for 10.10.10.10. Current addresses are 10.10.10.10,10.10.10.12.
  ```

  From this message, we know that the address used to establish the connection was 10.10.10.10. We also know that the system has two IP Addresses - 10.10.10.10, and 10.10.10.12.

  If the address 10.10.10.10 changes, we disconnect the connection, and log the following message:

  ```
  Adapter address changed from 10.10.10.10. Current addresses are 10.10.10.12, 10.10.10.13.
  ```

- CSCdy89047

  The VPN Client does not support Wireless LAN Ethernet cards.

- CSCdz10525

  The VPN Client, Release 3.6.2 for Solaris is not installable “remotely”. That is, the installation script does not do all of the installation and manipulation of files (in scripts like postinstall, postremove) via references to the BASEDIR and PKG_INSTALL_ROOT environment variables. For example, the script postinstall should never reference /etc/ (or any other directory) directly.

- CSCdz26371

  In a setup where a VPN Client behind a natted device connects to a VPN 3000 Concentrator using NAT-T (NAT Traversal), the VPN Client might fool the VPN Concentrator into thinking that the Concentrator is also behind a NAT device. The VPN Concentrator might therefore send keepalive packets to the VPN Client on destination port udp 4500. If this happens, the NAT device on the VPN Client side might drop the keepalive packets.

- CSCdz53527

  After executing the “vpnclient disconnect” command on a Linux or Mac VPN Client Release 3.7.2, the Linux VPN Client has a segmentation fault and the Mac VPN Client displays a paragraph concerning malloc and pointers.

  These harmless messages appear only if the command is used when the VPN Client is not actively connected.

- CSCdz58855

  Using the Mac OS X 10.2.2 with VPN Client, the VPN Client does not connect over a PPP interface.

- CSCdz62411

  The VPN Client does not show the session as disconnected after the VPN 3000 Concentrator terminates the session.

- CSCdz76732

  Using the Linux 3.7.2.12 VPN Client for Linux, version 3.7.2.12, the VPN Client locks up the workstation when trying to send traffic through the tunnel. Version 3.7.2.11 does not have this feature. This test was run on Linux RedHat 7.1, no NAT, no Certificates.

- CSCdz79677

  This affects the MacOS X GUI VPN Client, Release 3.7.2.

  If you do the following:

  1. Using one interface (e.g. wireless), make a VPN connection.

  2. Disconnect.

  3. Switch to a different interface (for example, wired).

  4. Attempt to reconnect.

  The connection fails (the login dialog never appears). If you quit and re-launch the VPN Client, the connection succeeds. The connection also succeeds if it's being made to a different server (the customer has six servers, and trying another site works).

- CSCdz86318

  While using the VPN Client for Macintosh, the first connection attempt after the workstation was in sleep mode fails to connect. This condition usually occurs in conjunction with a network interface change, such as having had the VPN Client connected over Ethernet before the sleep and over wireless after the sleep.

- CSCea11037

  While using the VPN Client on a Mac OS X workstation, the MTU of the interface gets lower and lower after a while of connecting the VPN Client after sleeping the workstation.

  This sometimes happens when a combination of factors align properly. The version of Mac OS X must be 10.1.x, the platform must be of older hardware, the switch interface negotiation must be slow (10 - 15 seconds), and the VPN Client must have been connected when the workstation was put to sleep.

  The VPN Client fails to recognize that the interface was lost (even though the VPN Client successfully disconnected when awakened) and does not readjust the MTU value back to its previous value. When the VPN Client makes its next connection, the MTU is lowered further.

- CSCea16072

  Using the Release 3.7.3 VPN Client on a Macintosh and previous versions on 10.2.1, the MTU is not lowered if the VPN Client connection was begun before DHCP was negotiated.

  If the workstation has the interface up but is still negotiating DHCP when the VPN Client connection is begun, the VPN Client stalls before it can contact the VPN 3000 Concentrator until the DHCP is complete. Then the VPN Client continues and connects successfully. The MTU, however, is still 1500.

  This could easily happen using a laptop when roaming and (depending on the timing of the connection and DHCP negotiation) could lead to intermittent problems caused by the MTU setting of 1500.

Caveats Resolved in Release 3.7.2

This section lists the caveats resolved in the Cisco VPN Client Release 3.7.2.

- CSCdx08823

  While using a VPN Client for Solaris, over a period of heavy traffic, the workstation locked up or panicked. This condition was usually caused by certain traffic types that unexpectedly caused problems with the workstations stack. The file transfer protocols NFS and SCP have been known to cause this issue.

- CSCdy44907

  In rare circumstances, users of the VPN Client for Solaris, Release 3.6, experienced system failures after creating a VPN tunnel and passing an indeterminate amount of traffic when running in 32- or 64-bit mode.

- CSCdy62769

  The certificate enrollment dialogue was very tall. On 800x600 screens, it was slightly larger than the desktop.

- CSCdy74476

  Text labels on buttons could not be clicked on. You had to click on the actual button icon.

- CSCdz03183

  The Simple GUI allowed resizing, but it should not do so.

- CSCdz12816

If the VPN Client disconnected, the MTU was not reset to its pre-connected value. For example, if the MTU was 1500 before the connection, the VPN Client reduced it to 1356 upon connecting. If the connection was lost, due to an interface going down or the Macintosh going to sleep, the MTU stayed at 1356, rather than being reset to 1500, as was expected.

- CSCdz13444

  Connection attempts using a VPN Client for Mac OS X failed when the VPN Concentrator was configured for load balancing.

  This condition appeared only when the VPN Client is attempting to connect using TCP NAT (TunnelingMode=1). This issue was introduced in Release 3.6.2; it had been working in previous versions. However, Mac OS X 10.2.x did not allow TCP NAT connections in previous versions and was limited in which interfaces were functional in earlier versions. Mac OS X 10.1.x is fully functional in earlier versions supporting Mac OS X.

- CSCdz25443

  IPSec over TCP (cTCP) worked inconsistently with Release 3.7 of the Cisco VPN Client when running on Mac OS X 10.2. You could usually get TCP to connect the first time you tried, but after that it would not connect unless you restarted the VPN Client. Tried this via dial-up and via broadband (wireless and wired).

- CSCdz27760

  Uninstaller from the Applications folder appeared to do nothing. Running the command line uninstaller failed with the following errors:

  ```
  [labusers-Computer:~] labuser% cd /Applications/Uninstall\ Cisco\ VPN\
  Client.app/Contents/MacOS/

  [labusers-Computer:Uninstall Cisco VPN Client.app/Contents/MacOS] labuser% ls

  Uninstall Cisco VPN Client

  [labusers-Computer:Uninstall Cisco VPN Client.app/Contents/MacOS] labuser% ls -l total 16

  -rwxrwxr-x  1 root  admin  6148 Nov  8 14:21 Uninstall Cisco VPN Client

  [labusers-Computer:Uninstall Cisco VPN Client.app/Contents/MacOS] labuser% ./Uninstall\
  Cisco\ VPN\ Client

  ./Uninstall Cisco VPN Client: Exec format error. Binary file not executable.

  [labusers-Computer:Uninstall Cisco VPN Client.app/Contents/MacOS] labuser% sudo
  ./Uninstall\ Cisco\ VPN\ Client

  Password:

  ./Uninstall Cisco VPN Client: ./Uninstall Cisco VPN Client: cannot execute binary file
  ```

- CSCdz48205

  VPN Client version 3.7.2did not support the ipdptp dialup interface on Solaris platforms. This ipdptp interface is used for dialup connections on the Solaris 6, 7, and 8 platforms. Solaris 8 can be upgraded with a standard patch from SUN. This allows them to use the new pppd 4.0 driver, which is still supported by the VPN Client. Newer Solaris 8 installations and Solaris 9 use pppd 4.0 as their standard dialup and PPoE driver.

Caveats Fixed in Previous Releases

The following sections list caveats fixed in previous releases of the VPN Client for Linux, Solaris, and Mac OS X.

Caveats Fixed in Release 3.7

- CSCdv66567, CSCdw15317

  Connection reliability issues no longer occur when you use the VPN Client for Mac OS X configured for cTCP NAT (TunnelingMode=1).
- CSCdw82857

  An unresolved symbol error no longer appears when the VPN Client builds the driver during the installation. Previously, this occurred because the get_fast_time function, required by the VPN Client, was removed from the Linux kernel API in the 2.4.18 release.
- CSCdw87223

  The VPN Client for Linux now binds only to supported interfaces (asynchronous serial PPP and Ethernet).
- CSCdx61265

  The VPN Client for Solaris install script now properly identifies the 10-MB Ethernet network interface and provides the correct entry in the /etc/iu.ap file.
- CSCdy38606

  When you install the VPN Client for Linux on a Mandrake Linux, the installer script now looks for the ID in the previous default location usr/bin/id and the new default location usr/id.
- CSCdy48192

  You can now configure a VPN Client for IPSec over TCP when running Mac OS Version 10.2.
- CSCdy49082

  The VPN Client now supports the new Linux distributions that use Version 3.2 + of the GCC compiler.
- CSCdy51818

  Split tunneling now functions properly for a VPN Client running Mac OS Version 10.2.
- CSCdy59183

  A VPN Client running Mac OS Version 10.2 no longer fails to connect to a VPN device if IPv6 is enabled.
- CSCdy81700

  You can now pass nontunneled traffic (other than ICMP) with split tunneling enabled on a VPN Client for Mac OS X and with OS Version 10.2.x on your workstation.

Caveats Fixed in Release 3.6.1

This section lists caveats fixed for the VPN Client in Release 3.6.1.

- CSCdv63980

  A VPN Client configured to use IPSec over TCP for NAT Transparency (TunnelingMode=1) can now use backup servers during connection attempts.

- CSCdv75911

  If you use a large certificate for authentication (such as one created by a Microsoft CA), a VPN Client configured to use IPSec over TCP for NAT Transparency (Tunneling Mode=1) can now establish a connection using PPP or Ethernet.

- CSCdv86123

  If you enroll certificates from a file and enter information in all fields, a segmentation fault no longer occurs.

- CSCdy41127

  The VPN Client now works correctly on interface en1 (Apple AirPort WiFi) card when running Mac OS Version 10.2.

Caveats Fixed in Release 3.5.1

This section lists caveats fixed for the VPN Client in Release 3.5.1.

- CSCdu66728, CSCdu66730, CSCdu66745, CSCdu66755

  If you issue the **cisco_cert_manager** command or any associated command operations, numerical error codes that cannot be interpreted without a translation table no longer appear.

- CSCdu76408

  The VPN Client for Linux can now establish a connection using certificates generated by a Microsoft Certificate Authority (CA).

- CSCdu78932

  The documentation for the VPN Client for Solaris has been updated to more accurately reflect the certificate enrollment process and now contains certificate troubleshooting tips.

- CSCdv43364

  The Simple Certificate Enrollment Protocol (SCEP) option is now available from the VPN Client **cisco_cert_mgr -E -op enroll** command.

- CSCdv53358

  The VPN Client can now use large certificates (such as one created by a Microsoft CA) over a PPP connection and when it is configured to use IPSec over TCP for NAT transparency.

- CSCdv53367

  The VPN Client can now pass large packets over a PPP connection if the client is configured to use IPSec over TCP or UDP for NAT transparency.

- CSCdv53430

  See CSCdu66728.

- CSCdv60435

  When you establish a VPN connection, legacy Mac OS applications can now pass traffic through the tunnel.

- CSCdv61653

  When you import a certificate, the password prompt now prompts you for an import password instead of a password to clarify which password to enter.
- CSCdv66465

  NFS file systems and directories are no longer unusable when the VPN Client is connected.
- CSCdv82220

  If IP masquerading is enabled on your workstation, you no longer experience difficulty using certain applications after the VPN Client is installed.
- CSCdv86262

  If you issue the **kill -9** command to the VPN Client or the cvpnd process, the tunnel is properly closed.
- CSCdv90944

  See CSCdu66728.
- CSCdw19659

  You can now make use of DNS servers to resolve names and perform lookup requests when the VPN Client is connected.
- CSCdw31304

  The value in the file ‘StartupParameters.plist’ is now a list instead of a string and subsequent startup items no longer fail to load.

Caveats Fixed in Release 3.5

This section lists caveats fixed for the VPN Client for Linux in Release 3.5.

Note Release 3.5. was the first release for the VPN Client supporting the Mac OS X and Solaris operating systems.

- CSCdu36896

  The VPN Client can now upload large packets to a VPN 3000 concentrator over a PPP or Ethernet connection if NAT transparency is enabled on both ends of the tunnel.
- CSCdu58641

  If the VPN Client is shut down improperly, the **/etc/rc.d/init.d/vpnclient_init stop** command now correctly unloads the client kernel module.
- CSCdu66280

  During the installation process, the VPN Installer now correctly unloads a currently running VPN module.
- CSCdu66791

  FTP downloads performed using IPSec/UDP are no longer slower than FTP downloads performed using IPSec Protocol 50 (ESP).

- CSCdu66993

  The VPN Client no longer becomes inoperable if your Version 2.4 kernel is compiled with CONFIG_NETFILTER enabled.
- CSCdu67913

  Systems behind a device using port address translation (PAT) are now able to access web pages when the VPN Client is loaded on a workstation, but not in use.
- CSCdu81881

  The host name on the computer running the VPN Client is now resolved in DNS. Previously, this occurred on a Mandrake Version 8.0 system running Version 2.4.7 kernel.
- CSCdu82424

  The VPN Client module is now built properly on Redhat Version 7.1.
- CSCdv04430

  When you use the VPN Client with Redhat Version 6.2 with the Enable Backup feature enabled, you can now pass traffic when it is redirected to a backup server or a load balancing server.
- CSCdv10084, CSCdv13171

  When LZS Compression is enabled on the VPN Client, DNS names are resolved and you can access internal web pages.
- CSCdv49427

  The VPN Client now has the capability to fragment large certificates and establish an IPSec over TCP connection with a VPN 3000 concentrator using Software Version 3.5.

Open Caveats

The following sections describe known issues for the VPN Client Version 3.7.3.

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

http://www.cisco.com

Translated documentation is available at this URL:

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

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped 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 through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/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 Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

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

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

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

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

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

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

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

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

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

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

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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