Release Notes for the Cisco VPN Client Version 3.5.1 for Linux, Solaris, and Mac OS X

February 4, 2002

These release notes provide information about the Cisco VPN Client Version 3.5.1 for Linux, Solaris, and Mac OS X. These release notes are updated as needed to describe new and changed information, caveats, and documentation updates.

Please read the release notes carefully prior to installation.

This document applies to the following operating systems:

- Linux for Intel
- ultraSPARC Solaris
- Macintosh OS X

Contents

This document contains the following sections:

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

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.
- ultraSPARC computer running a 32-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 VPN 3000 Concentrator Series, Version 3.0.x and later.
- Cisco PIX Firewall Version 6.1(1) and later.

Caveats Fixed in This Release

This section describes the caveats fixed in the Cisco VPN Client Version 3.5.1 for Linux, Solaris, and Mac OS X.

Caveats Fixed for Linux

- 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, CSCdv53430, CSCdv90944

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

- CSCdv43364

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

- 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.

- CSCdv61653

  When you import a certificate, the password prompt nows asks 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 poperly closed.

Caveats Fixed for Solaris

- 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.

- 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.

Caveats Fixed for Mac OS X

- CSCdv60435

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

  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 Previous Releases

This section describes caveats fixed in Version 3.5.0 of the VPN client for Linux.

- 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 (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 you have the VPN client loaded on your workstation, but you are not using it.

- CSCdu81881

  The hostname 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 EnableBackup feature enabled, you can now pass traffic when 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 3.5.1.

Open Caveats for Linux

This section lists open caveats for the VPN client Version 3.5.1 for Linux.

- 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 should appear 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.

Open Caveats for Mac OS X

This section lists open caveats for the VPN client Version 3.5.1 for Mac OS X.

- CSCdv63980

  The VPN client is unable to use backup servers during connection attempts if it is configured to use IPSec over TCP for NAT transparency (**TunnelingMode=1**).

  Workaround: Configure the VPN client profile to use IPSec over UDP for NAT transparency (**TunnelingMode=0**) or disable the backup server **(EnableBackup=0)**.

- CSCdv75911

  If the VPN client is configured to use IPSec over TCP for NAT transparency (**TunnelingMode=1**), you cannot establish a connection using PPP or Ethernet if you use a large certificate (such as one created by a Microsoft CA).

  Workaround 1: Use a CA that creates smaller certificates.

  Workaround 2: If you are using an Ethernet connection, configure the VPN client to use IPSec over UDP for NAT transparency (**TunnelingMode=0**).

- CSCdv86123

  If you are using the enroll command for certificates and you enter information in all fields, you might get a segmentation fault.

  Workaround: Enter only the required fields (cn, caurl, and cadn) when enrolling certificates.

Open Caveats for Solaris

This section lists open caveats for the VPN client Version 3.5.1 for Solaris.

- CSCdw27781

  If you have an IP firewall 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 vpnclient kernel module cipsec and the ipfilter firewall module.

  Workaround: Disable the ipfilter firewall kernel module *before* you install the VPN client.

Limitations

This section lists limitation for the VPN client Version 3.5.1 for Solaris.

- CSCdv75825

  If the VPN client uses routed RIP to learn its default route, you might lose connectivity. This is because RIP is blocked when the VPN client is connected in all tunneling mode.

  No workaround.

Obtaining Documentation

The following 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 the following URL:

http://www.cisco.com

Translated documentation is available at the following 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

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, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Cisco Systems
Attn: 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 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 to

- 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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

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

Inquiries to Cisco TAC 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.

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

Cisco TAC Web Site

The Cisco TAC Web Site allows you 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 the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services 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 the following URL to register:

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

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

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; 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 will automatically open a case.

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

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

Before calling, please 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). In addition, please have available your service agreement number and your product serial number.