Release Notes for Cisco VPN 3002 Hardware Client, FIPS Release 3.1.3

CCO March 19, 2002

Introduction

Note You can find the most current documentation for the Cisco VPN 3002 on CCO.

These release notes are for the Cisco VPN 3002 Hardware Client, FIPS Release, which is based on Release 3.1.3 software. These release notes describe limitations and restrictions, caveats, and related documentation. Read the release notes carefully prior to installation.

The Cisco VPN 3002 Hardware Client (referred to in these Release Notes as the VPN 3002) communicates with a VPN 3000 Series Concentrator to create a virtual private network across a TCP/IP network (such as the Internet). The VPN 3002:

- Provides an alternative to deploying the VPN Client at remote locations.
- Is located at a remote site (like the VPN Client).

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

- Provides a secure connection to a VPN Concentrator at a central site.
- Requires minimal configuration.

The secure connection between the VPN 3002 and the VPN Concentrator is called a *tunnel*. The VPN 3002 uses the IPSec protocol to negotiate security parameters, create and manage tunnels, encapsulate packets, transmit or receive them through the tunnel, and unencapsulate them. It can support a single IP network.

The VPN 3002 Hardware Client provides an alternative to deploying the VPN Client software to PCs at remote locations. Like the software client, the VPN 3002 is located at a remote site, and provides a secure connection to a VPN Concentrator at a central site. It is important to understand that the VPN 3002 is a hardware *client*, and that you configure it as a client, not as a site-to-site connection.

Contents

These release notes supplement the Security Policy document and include the following topics:

System Description, page 3

Installation Notes, page 4

Caveats, page 5

Documentation Updates, page 7

Service and Support, page 9

Obtaining Documentation, page 9

Obtaining Technical Assistance, page 11

System Description

The following sections describe the VPN 3002 hardware.

Physical Site Requirements

The VPN 3002 requires a normal computing-equipment environment, including power requirements. For maximum protection, we recommend connecting it to a conditioned power source or UPS (uninterruptible power supply). Be sure that the power source provides a reliable Earth ground.

Physical Specifications

- Width: 8.85 inches (22.48 cm)
- Depth: 7 inches (17.78 cm)
- Height: 2.12 inches (5.38 cm)
- Weight: 2.25 lb. (1.02 kg)
- External power supply:
  - Input: 100 to 240 VAC at 50/60 Hz (autosensing)
  - Output: 3.3 v @ 4 amps
- Cooling: Normal operating environment, 32^{o} to 122^{o}F (0^{o} to 50^{o}C), convection only; cooling intake vents are on the sides and top. Allow at least 3 inches (75 mm) of unobstructed space on all sides.
- Cabling distances from an active network device: approximately 328 feet (100 meters)
- UL approved: electrical, mechanical, and construction
- FCC, E.U., and VCCI Class B compliance

Installation Notes

For complete installation information, refer to the *VPN 3002 Hardware Client Getting Started* guide. To install and configure the VPN 3002 using default values, see the *VPN 3002 Quick Start* card, which ships with the VPN 3002.

Browser Requirements

The FIPS version of the VPN 3002 Hardware Client Manager works with the following browsers:

- Netscape version 6.1 or greater
- Internet Explorer 5.0 or greater with 128-bit cipher-strength

Be sure JavaScript and cookies are enabled in the browser. Whatever browser and version you use, install the latest patches and service packs for it.

Do not use the *browser* navigation toolbar buttons **Back, Forward**, or **Refresh / Reload** with the VPN 3002 Hardware Client Manager unless instructed to do so. To protect access security, clicking **Refresh / Reload** automatically logs out the Manager session. Clicking **Back** or **Forward** may display stale Manager screens with incorrect data or settings.

We recommend that you hide the browser navigation toolbar to prevent mistakes while using the VPN 3002 Hardware Client Manager.

Recommended PC Monitor/Display settings

For ease of use, we recommend setting your monitor or display:

- Desktop area = 1024 x 768 pixels or greater. Minimum = 800 x 600 pixels.
- Color palette = 256 colors or higher.

Online Documentation

The online documentation might not be accessible when using Internet Explorer with Adobe Acrobat**:** Version 3.0.1. To resolve this issue, upgrade to Acrobat 4.0, which is available at the Adobe web site: http://www.adobe.com.

Password Maintenance

Be aware that there is no way to recover your system if you forget the Administrator password. Take appropriate measures to safeguard your password and remember it. If you forget the Administrator password, you cannot log in to your system and you will have to return the VPN Concentrator to be recovered.

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases. Severity 1 caveats are the most serious caveats; severity 2 caveats are less serious.

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 Innovator II on CCO, select Software & Support: Online Technical Support: Software Bug Toolkit or navigate to http://www.cisco.com/support/bugtools.

Open Caveats

The following problems exist with VPN 3002 Hardware Client, FIPS Release 3.1.3.

- CSCds75601

  The VPN 3002 DHCP server does not restore DHCP leases after the VPN 3002 reboots. DHCP clients must renew their leases to populate the VPN 3002 DHCP server.

- CSCdt21080

  Unable to unlock a locked configuration

  If you are managing a device and do not log out properly, the configuration file is locked by any other IP Address of the managing device until that session expires.

  For a VPN Concentrator, you can physically log out this admin user, but with a VPN 3002, the problem persists until the session expires (the default is 10 minutes) or you reboot the unit.

- CSCdt38841

  The VPN 3002 DHCP server may at times assign addresses that are not in sequence, skipping addresses that are free for use.

- CSCdt42173

  The VPN Concentrator family of products does not support SSH connections from TeraTerm SSH version: TTSSH v1.2/TTPRO v2.3. If you plan to use SSH from TeraTerm, and are currently running this version, visit the following site and upgrade your SSH software: http://www.zip.com.au/~roca/ttssh.html

- CSCdt42408

  The MS Exchange/Outlook auto-update feature doesn't work in Client (PAT) mode. There is an open Microsoft bug for this problem.

- CSCdt42421, CSCdu57252

  The Traceroute debugging tool does not work from a device on the private LAN of a VPN 3002.

- CSCdt48908

  When changing IP addresses (from static to DHCP mode and vice-versa) on the VPN 3002 public interface, data starts passing approximately 30 seconds after the tunnel to the central-site VPN 3000 has been established.

- CSCdt49326, CSCdu57255

  When the VPN 3002 is configured for 10 Mbps and the duplex mode is configured for auto, the duplex mode may be incorrectly displayed in the Monitor | Statistics | MIB II | Interfaces | Ethernet screen as "half" duplex even though it is running at "full" duplex.

- CSCdu50355

  When you view the VPN 3002 ARP table with PPPoE enabled, entries for Interface 12 appear. Interface 12 is currently being used as the PPPoE interface.

- CSCdu52733

  When the route table for a VPN 3002 with PPPoE enabled is displayed on either the CLI or HTML interface, the following route appears in the table. Ignore it.

```
Address         Mask          Next Hop         Int
0.0.0.0      255.0.0.0       0.0.0.0       public in
```

- CSCdu66046

  On a VPN 3002 configured for PAT mode, after an IPSec rekey occurs, the Assigned IP Address field does not display on the System Status window.

- CSCdv37212

  When a VPN 3002 uses a DNS name for the connection, the VPN 3002 may be unable to reconnect after a rekey.

- CSCdv72871

  The VPN 3002 does not accept a DHCP address when the relay device sets unicast_ DHCPOFFER packet with the broadcast flag set.

Documentation Updates

The Cisco VPN 3002 documentation set has not been revised for this release. However, the standard documentation is available online through Cisco Connection Online (CCO).

On-line Context Sensitive Help Differences

Many differences exist between the FIPS-compliant Release and the online help. This section lists the most important differences.

- Throughout the VPN Hardware Client Manager's browser interface, parameters that are not FIPS compliant have been labeled **(Non FIPS)**.

- Throughout the VPN Hardware Client Manager, the toolbar on the third line of the screen contains the tab: **Check FIPS Compliance**. Clicking on this tab takes you to the **Configuration | FIPS Compliance** page, which has a help page that explains how to configure the VPN 3002 to be FIPS compliant.
- The list of events contains two new event classes, FIPS and FIPSDIAG. These classes appear in the list on the **Configuration | System | Events | Classes | Add/Modify** screen.
- The Reboot option on the **Administration | System Reboot** page is **Reboot/Zeroize (Deletes all keys and security parameters)**.

Some of the online help pages do not accurately reflect the default values for FIPS operation. The following list provides the correct default values.

- HTTP/HTTPS: HTTP is disabled, and HTTPS is enabled.
- Telnet: Both Telnet and Telnet/SSL are disabled.
- SSL
  - Encryption Protocols: 3DES-168/SHA, DES-56/SHA, DES-40/SHA Export
  - SSL Version: TLS V1 with SSL V2 Hello
- SSH Encryption Protocols: 3DES-168, DES-56
- General Events severity to console is None
- Event Classes severity to console is None
- Access Settings: Configure File Encryption is DES.

Command-Line Interface Limitations

This section lists some limitations and differences in the way the command-line interface operates on the VPN 3002.

- You cannot access the file system from the command-line interface; however, you can access the file system through the browser interface using HTTPS.
- The Event log viewer is not accessible through the command-line interface.
- The software update feature is not accessible through the command-line interface; however you can access the software update feature through the browser interface using HTTPS.

Service and Support

For service and support for a product purchased from a reseller, contact the reseller, who offers a wide variety of Cisco service and support programs described in "Service and Support" in the *Cisco Information Packet* shipped with your product.

Note If you purchased your product from a reseller, you can access CCO as a guest. CCO is Cisco Systems' primary real-time support channel. Your reseller offers programs that include direct access to CCO services.

For service and support for a product purchased directly from Cisco, use CCO.

Software Configuration Tips on the Cisco TAC Home Page

The Cisco TAC home page includes technical tips and configuration information for the VPN 3002 Hardware Client. Find this information at:

http://www.cisco.com/warp/public/707/index.shtml#vpn3000

and scroll down to the section, "Cisco VPN 3000 Concentrator."

Obtaining Documentation

This section describes how to obtain the documentation on the Web or how to access the documentation on CD-ROM.

Note Except for these Release Notes, no printed documentation ships automatically with this product. Please see the following sections for information about obtaining documentation for this product and for other Cisco products.

VPN 3002 Hardware Client Documentation

VPN 3002 documentation for FIPS includes the following:

- VPN 3002 Hardware Client Security Policy document. This document is available online only.
- The *VPN 3002 Hardware Client Getting Started* manual provides information to take you from unpacking and installing the VPN 3002, through configuring the minimal parameters to make it operational (called Quick Configuration). This manual is online only.
- The *VPN 3002 Hardware Client Reference* provides details on all the functions available in the VPN 3002 Hardware Client Manager. This manual is online only.
- The HTML interface, called the VPN 3002 Hardware Client Manager, includes extensive context-sensitive online help that you can access by clicking the **Help** icon on the toolbar in the Manager window.
- The *VPN 3002 Hardware Client Quick Start* card summarizes information for Quick Configuration. This quick reference card is provided with the VPN 3002, and is also available online. For easiest use, print it on 8 1/2" x 11" paper, in duplex mode.
- The *VPN 3002 Hardware Client Basic Information* sticky label summarizes information for installing the VPN 3002 and beginning configuration. We suggest that you can affix the label to the VPN 3002 as a ready reference. You can also print a copy of the label from the online version. Current customers who obtain version 3.1 software from CCO can also order the 3.1 version of the label from CCO. When ordering the label, use product number CVPN3002-LABEL-31=.

World Wide Web

Documentation for this product and for all Cisco products is available on the World Wide Web. You can access the most current Cisco documentation at: http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Ordering documentation

Cisco documentation and additional literature are available in a CD-ROM package, which is available as a single unit or as an annual subscription. Registered CCO users can order the Documentation CD-ROM and other Cisco Product documentation through our online Subscription Services at: http://www.cisco.com/cgi-bin/subcat/kaojump.cgi.

Nonregistered CCO users can order documentation through a local account representative by calling Cisco's corporate headquarters (California, USA) at 408 526-4000 or, in North America, call 800 553-NETS (6387).

Obtaining Technical Assistance

Cisco provides Cisco Connection Online (CCO) as a starting point for all technical assistance. Warranty or maintenance contract customers can use the Technical Assistance Center. All customers can submit technical feedback on Cisco documentation using the web, e-mail, a self-addressed stamped response card included in many printed docs, or by sending mail to Cisco.

Cisco Connection Online

Cisco continues to revolutionize how business is done on the Internet. Cisco Connection Online 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.

CCO's broad range of features and services helps customers and partners to streamline business processes and improve productivity. Through CCO, you will find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online support services, 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 CCO to obtain additional personalized information and services. Registered users can order products, check on the status of an order and view benefits specific to their relationships with Cisco.

You can access CCO in the following ways:

- WWW: www.cisco.com
- Telnet: cco.cisco.com
- Modem using standard connection rates and the following terminal settings: VT100 emulation; 8 data bits; no parity; and 1 stop bit.
  - From North America, call 408 526-8070
  - From Europe, call 33 1 64 46 40 82

You can e-mail questions about using CCO to cco-team@cisco.com.