Release Notes for Cisco VPN 3002 Hardware Client Release 3.5.2

These release notes describe the features of the Cisco VPN 3002 Hardware Client and the caveats that apply for Release 3.5.2. Read the release notes carefully prior to installation.

Contents

These release notes include the following topics:

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

Introduction

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).
- Provides a secure connection to a VPN 3000 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 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.

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.

Initial Configuration

You must meet the following requirements to configure the VPN 3002.

Central-site VPN Concentrator Requirements

To interoperate with a VPN 3002, the VPN 3000 Series Concentrator to which it connects must:

- Be running software version 3.0 or later. For most features new in software version 3.5, you must be running version 3.5 software on both the VPN 3002 and on the VPN Concentrator to which it connects.
- Configure IPSec group and user names and passwords for this VPN 3002.
- For a VPN 3002 running in PAT mode, enable a method of address assignment: DHCP, address pools, per user, or authentication server address.
- For a VPN 3002 running in Network Extension mode, use Reverse Route Injection, a VPN Concentrator feature new in Release 3.5, or configure on your central-site router a static route to the private network of the VPN 3002.

See Chapter 3, "Quick Configuration using the VPN 3002 Hardware Client Manager," in the *VPN 3002 Hardware Client Getting Started* manual for step-by-step Quick Configuration instructions.

Release 3.5 New Software Features

The following sections describe software features new in Release 3.5.

IPSec over TCP

IPSec over TCP encapsulates encrypted data traffic within TCP packets. This feature enables the VPN 3002 to operate in an environment in which standard Encapsulating Security Protocol (ESP, Protocol 50) or Internet Key Exchange (IKE, UDP 500) cannot function, or can function only with modification to existing firewall rules. IPSec over TCP encapsulates both the IKE and IPSec protocols within a TCP packet, and enables secure tunneling through both NAT and PAT devices and firewalls.

Note This feature does not work with proxy-based firewalls.

The VPN 3002 Hardware Client, which supports one tunnel at a time, can connect using either standard IPSec, IPSec over TCP, or IPSec over UDP.

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

Interactive Hardware Client Authentication

Interactive hardware client authentication provides the central site with additional security by requiring the VPN 3002 to authenticate with a username and password that you enter manually each time the VPN 3002 initiates a tunnel. With this feature enabled the VPN 3002 does not have a saved username and password.

When the VPN 3002 initiates the tunnel, it sends the username and password to the VPN Concentrator to which it connects. The VPN Concentrator facilitates authentication on either the internal or an external server. If the username and password are valid, the tunnel is established.

You configure interactive hardware client authentication on a group basis on the VPN Concentrator at the central site, which then pushes the policy to the VPN 3002.

Individual User Authentication

Individual user authentication protects the central site from access by unauthorized persons on the same LAN as the VPN 3002.

When you enable individual user authentication, each user that connects through a VPN 3002 must open a web browser and manually enter a valid username and password to access the network behind the VPN Concentrator, even though the tunnel already exists.

Note You cannot use the command-line interface to log in if user authentication is enabled. You must use a browser.

- If your browser points to a default home page, or to a website on the remote network behind the VPN Concentrator, the VPN 3002 directs the browser to the proper pages for user login. When you successfully log in, the browser displays the page you originally entered.

- If you try to access resources on the network behind the VPN Concentrator that are not web-based, for example, email, the connection will fail until you authenticate.
- To authenticate if your browser does not automatically redirect you to the login pages, enter the IP address for the private interface of the VPN 3002 in the browser Location or Address field. The browser then displays the login screen for the VPN 3002. To authenticate, click the Connect/Login Status button.

You configure individual user authentication on a group basis on the VPN Concentrator at the central site, which then pushes the policy to the VPN 3002.

RADIUS with Password Expiry

RADIUS with password expiry is an IPSec authentication method that you configure on a VPN Concentrator on a group basis. This option lets the VPN 3000 Concentrator that is attempting to authenticate an IPSec client to an external RADIUS server (acting as a proxy to an NT server) determine when a user’s password has expired and prompt for a new password. By default, this option is disabled.

Enabling this option allows the VPN 3000 Concentrator to use MS-CHAP-v2 when authenticating an IPSec client to an external RADIUS server. That RADIUS server must support both MS-CHAP-v2 and the Microsoft Vendor Specific Attributes. Refer to the documentation for your RADIUS server to verify that it supports these capabilities.

Because of the use of MS-CHAP-v2, when this option is enabled on the VPN 3000 Concentrator, the VPN Concentrator can provide enhanced login failure messages that describe specific error conditions. These conditions are:

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

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

Note To use RADIUS password expiry with a VPN 3002, you must enable interactive hardware client authentication. This feature does not work for individual user authentication.

Backup IPSec Servers

IPSec backup servers let a VPN 3002 Hardware Client connect to the central site when its primary central-site VPN Concentrator is unavailable. You configure backup servers for a VPN 3002 either on the VPN 3002 or on a group basis at the VPN Concentrator. If you configure backup servers on the central-site VPN Concentrator, that VPN Concentrator pushes the backup server list to the VPN 3002 hardware clients in the group.

Load Balancing

Load balancing lets you distribute sessions among two or more VPN Concentrators connected on the same network to handle remote sessions. Load balancing directs sessions to the least loaded device, thus distributing the load among all devices. It makes efficient use of system resources and provides increased performance and high availability. Load balancing requires no configuration on the VPN 3002.

Simple Certificate Enrollment Protocol (SCEP)

You can enroll and install digital certificates on the VPN 3002 automatically or manually. The automatic method is a new feature that uses the Simple Certificate Enrollment Protocol (SCEP) to streamline enrollment and installation. SCEP is a secure messaging protocol that requires minimal user intervention. This method is quicker than enrolling and installing digital certificates manually, but it is available only if you are both enrolling with a CA that supports SCEP and enrolling via the web. If your CA does not support SCEP, or if you enroll with digital certificates by a means other than the web (such as through email or by a diskette), then you cannot use the automatic method; you must use the manual method.

Reset/Restore Monitoring Statistics

You can now reset and restore statistical data to better note changes in that data. When you click Reset on a monitoring or administration screen, the VPN 3002 temporarily resets a counter for the chosen statistics without affecting the operation of the device. You can then view statistical information without affecting the actual current values of the counters or other management sessions. The function is like that of a vehicle’s trip odometer, versus the regular odometer. Click Restore to return to the actual statistical values.

XML Management

VPN 3000 Concentrators and VPN 3002 Hardware Clients now support an XML-based interface to allow them to be more easily managed by an external management application.

This interface can be used by Cisco management applications, third-party applications that manage our products, and customers who want to manage their devices using their own infrastructure. This feature is enabled my default; you do not have to configure it.

The XML data can be sent to or uploaded from the VPN 3000 Concentrator using HTTPS, SSH, or standard file transfer mechanisms such as FTP or TFTP.

Reverse Route Injection (RRI)

You can configure the VPN 3000 Concentrator to add routes to its routing table for remote hardware or software clients. The VPN Concentrator can then advertise these routes to its private network via RIP or OSPF. This feature is called reverse route injection (RRI).

For example, with a VPN 3002 in network extension mode, network extension RRI automatically adds hosts on the VPN 3002 private network to the VPN Concentrator’s routing table for distribution by either RIP or OSPF.

RRI requires no configuration on the VPN 3002.

Limitations and Restrictions

This section lists the issues to consider before installing Release 3.5.2 of the VPN 3002 Hardware Client software.

Disable SNMP for VPN 3002 Hardware Client Software Versions Before Release 3.5.2

In versions earlier than Release 3.5.2, an error can occur with management protocol processing (CSCdw65903). See the following URL for further information:
http://www.cisco.com/cgi-bin/bugtool/onebug.pl?bugid=CSCdw65903

In software versions prior to Release 3.5.2, this issue existed on both the public and private interfaces of the VPN 3002. However, the default configuration for the VPN 3002 enables SNMP only on the private interface; this reduces exposure to this problem.

To eliminate this issue from both the public and private interfaces, if you do not upgrade to Release 3.5.2, you must disable SNMP on both the public and private interfaces. To do this, go to the screen Configuration | System | Management Protocols | SNMP and deselect “Enable”.

If you do not want to disable SNMP on the entire VPN 3002, you can minimize exposure to this problem by ensuring that SNMP is disabled on the public interface. To do this, verify that no rule to allow SNMP traffic has been added to the public interface.

Release 3.5.2 resolves this issue.

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 or higher. The latest version of Adobe Acrobat is available at the Adobe web site: http://www.adobe.com.

Internet Explorer 4.x Browser

The following are known issues with Internet Explorer 4.X and the VPN 3002 Hardware Client Manager (the HTML management interface). To avoid these problems, use the version of Internet Explorer on the Cisco VPN 3002 software distribution media.

- If you encounter a script error when you try to save your configuration file using Internet Explorer 4.0, reinstall Internet Explorer 4.0, or upgrade to a later version of Internet Explorer. Reinstalling Internet Explorer fixes the problem.
- If you plan to upgrade the firmware on multiple VPN Concentrators at the same time from the same PC, use the version of Internet Explorer on the Cisco VPN 3000 software distribution media or newer. Using an earlier version could cause a failure in one or more of the upgrades.

Secure Management Using SSL

- When connecting to the VPN 3002 using SSL with Internet Explorer 4.0 (v4.72.2106.8), you might receive a message box saying, “This page contains both secure and non-secure items. Do you want to download the non-secure items?” Select Yes. There really are no *non-secure* items on the page and the problem is with Internet Explorer 4.0. If you upgrade to Internet Explorer 4.0 Service Pack 1 or Service Pack 2, you should not see this error message again.
- After adding a new SSL certificate, you might have to restart the browser to use the new certificate.

Some Data Is Not Tracked With Interactive Hardware Client Authentication and Individual User Authentication Enabled

If you are using an Accounting Server with Interactive Hardware Client Authentication and Individual User Authentication enabled, some session information specific to the level of data activity (number of octets and packets sent and received) back to the Accounting Server is not tracked (CSCdv82830).

Note This information *is* tracked if the Interactive Hardware Client is not enabled.

Caveats

Caveats describe unexpected behavior or defects in Cisco software releases.

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, 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, Release 3.5.

- CSCdt38841

  The VPN 3002 DHCP server sometimes assigns addresses that are not in sequence, skipping addresses that are free for use.

- CSCdt42421, CSCdu57252

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

- 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 as "half" duplex even though it is running at "full" duplex.

- CSCdv27743

  Using the rekey option to renew an SSL certificate from the RSA CA results in a rejection of the request.

  The resubmit/renew feature does work with RSA as long as the certificate being rekeyed or renewed is first deleted from the CA database. RSA does not allow a CA to issue more than 1 certificate with any particular DN.

- CSCdv50669

  If there are more than 150 networks in a network list used for split tunneling on the central site VPN Concentrator, when a VPN 3002 connects to the VPN Concentrator using this group and attempts to establish an SA to all of the networks within that network list, it may cause a reboot. We recommend that a network list that applies to a VPN 3002 contain 150 or fewer networks.
- CSCdv66367

  The VPN 3002 experiences an exception when the static route, default route, or interface setting is deleted/modified.
- CSCdv69320

  With an active tunnel between a VPN 3002 and VPN Concentrator, occasionally the event `IPSec input- discarding pkt with no NAT Rule` displays. No negative operational issues have been noted when this happens.
- CSCdv72871

  VPN 3002 does not accept a DHCP address when the relay device sets unicast_ DHCPOFFER packet with the BROADCAST flag SET.
- CSCdv85725

  When using Challenge-based authentication such as New PIN mode for SDI, the command-line interface does not present the question or reply text. The workaround is to use the HTML interface.
- CSCdv86086

  The Nexland router has problems with IKE Phase-1 rekeying. When this happens the 3002 tunnel disconnects. Data movement brings up the tunnel again.
- CSCdw20486

  The Cisco SoundStation Premier (Polycom IP Speaker Phone) is unable to get a valid DHCP IP Lease from the 3002s integrated DHCP server.
- CSCdw47278

  If the public interface uses PPPoE and the peer address is entered as a name rather than an IP address, DNS resolution fails; therefore the tunnel does not establish.

- CSCdw69363

  When Netscape Navigator or Internet Explorer is configured for auto proxy configuration and you use the browser to try to log in as a user to the VPN 3002, the web redirect tries to set up the proxy settings for the browser.

- CSCdw77824

  If a VPN 3002 cannot establish a tunnel to the central-site Concentrator, it keeps trying to connect. This can cause sufficient traffic to result in denial of service for other VPN clients during peak traffic hours. The probable cause is a configuration error. The workaround is to disconnect the VPN 3002 and correct the configuration.

Obtaining Documentation

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

VPN 3002 Documentation

VPN 3002 documentation includes the following:

- 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. Current customers who obtain version 3.5 software from CCO can also order the 3.5 version of the card from CCO. When ordering the card, use product number DOC-????.
- 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 3.5 software from CCO can also order the 3.5 version of the label from CCO. When ordering the label, use product number CVPN3002-LABEL-35=.

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, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
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.