Cisco Secure VPN Client Version 1.1 Quick Start Guide

Thank you for purchasing the Cisco Secure VPN Client. The Cisco Secure VPN Client is a component of Cisco Secure VPN Software, and an integral part of the Cisco Systems' family of hardware and software IPSec VPN solutions. Its robust implementation of IPSec standards allows remote Windows 95, Windows 98, and Windows NT 4.0 users to easily create secure and reliable VPN tunnel connections to a host network. Its features include support for DES and Triple DES encryption, authentication with digital certificates, one-time password tokens, pre-shared keys, Registration Authority (RA) & Certification Authority (CA) certificate enrollment protocol (CEP), and extended authentication (XAUTH), and is designed to fully complement Microsoft's TCP/IP implementation.

In addition to the quick start guide, this package contains the software license agreement and the Cisco Secure VPN Client installation CD-ROM.

Audience

Read this quick start guide if you are the network administrator who is responsible for defining network security policies and distributing them to the end users within your organization.

Note You will need digital certificates from a certification authority (CA), for example, Windows 2000 Certificate Services, Entrust, Netscape, or VeriSign, to implement secure communications with this software. Because each CA handles requests differently, you should contact the CA of your choice for detailed instructions on how to submit and receive certificate requests *before* you install this software.

System Requirements

- PC-compatible Computer—Pentium processor or equivalent
- Operating System—Microsoft Windows 98, Microsoft Windows 95, or Microsoft Windows NT 4.0 (with Service Pack 3, 4, 5 or 6)
- Minimum RAM—16 MB RAM for Windows 95, 32 MB RAM for Windows 98 or Windows NT 4.0
- Available Hard Disk Space—Approximately 9 MB
- Software Installation—CD-ROM drive
- Interoperability Requirements—See the latest C*isco Secure VPN Client Release Notes* at the following URL on CCO[1]:

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnrn/index.htm
- Communications Protocol—Native Microsoft TCP/IP
- Dial-up Connections—Modem, internal or external, non-encrypting, or Native Microsoft PPP dialer
- Network Connections—Ethernet

1. See the “Cisco Connection Online” section for more details.

Installing Cisco Secure VPN Client

Note If your operating system is Windows NT, you must have administrator privileges on your computer to install Cisco Secure VPN Client.

To install Cisco Secure VPN Client:

1. With Microsoft Windows running, make sure all other programs are closed before continuing.
2. Insert the Cisco Secure VPN Client CD-ROM. If it does not start automatically, do the following:
   a. From the **Start** menu, choose **Run**.
   b. Type **`d:\setup.exe`** (The *d* designates your CD-ROM drive, which could be different depending on your computer's setup).
   c. Click **OK**.
3. When the installation wizard starts, follow the instructions on your screen.

4. When setup has finished, click **Yes, I want to restart my computer now**.
5. Remove the CD-ROM, then click **Finish**. Your computer will automatically restart.
6. The SafeNet icon now appears in the status area of your Windows taskbar, which is usually located in the lower right corner of your screen.

   The SafeNet icon changes color and image as you begin and end communications. For more information, search for *SafeNet icon* in the Cisco Secure VPN Client help file.

Roles in Cisco Secure VPN Client Operation

For end users, Cisco Secure VPN Client starts automatically each time the computer starts, and runs transparently at all times behind other software applications.

For network administrators, you need to know how to perform the following tasks so that you can configure a custom installation for your end users:

- Requesting, importing, and exporting digital certificates and keys using the Cisco Secure VPN Client Certificate Manager
- Configuring and exporting security policies using the Cisco Secure VPN Client Security Policy Editor

Additional Information

Once you have Cisco Secure VPN Client installed on your computer, you will need to follow the outline in the next section, “Configuring a Custom Installation”, to configure a custom installation for your end users. Remember that this is only an outline. You will need to refer to the Cisco Secure VPN Client help file for step-by-step instructions.

Note If you cannot find the answers to your questions in the help file, contact your authorized product distributor.

To open the help file:

- Right-click the SafeNet icon. From this menu, click **Help**.

  or

- In the Security Policy Editor, click the **Help** menu. From the Help menu, click **Contents and Index**.

Configuring a Custom Installation

This outline directs you to the Cisco Secure VPN Client help topics that are listed under the **Contents** tab in the left pane.

Obtaining Digital Certificates

Double-click the “Working with Digital Certificates” book for a list of topics that help you determine the following tasks:

- Requesting your CA's digital certificate and importing it into Certificate Manager
- Requesting your own digital certificate and importing it into Certificate Manager. In this case, you will be requesting personal certificates for your end users.

Exporting Digital Certificates

Double-click the “Working with Digital Certificates” book, then double-click the “Exporting Digital Certificates and Keys” book. Click the “Export a personal certificate with keys and CA certificate” topic for instructions.

Configuring a Security Policy

Double-click the “Configuring Connections” book and “Configuring Security Policies” book for lists of topics. Determine whether you will keep the default security policy that is already defined in Security Policy Editor, or if you will customize it for your end users. This also means that you can configure different security policies for individual departments or end users within your organization.

Exporting a Security Policy

Double-click the “Configuring Security Policies” book. Follow instructions from the “Export a security policy” topic and note these changes:

- Disregard the note about **My Identity** and importing the file. You are taking care of this by customizing an installation.
- Enter the following filename, not the default filename, exactly as it appears here:

  `IPSecPolicy.spd`

Distributing Files to Your End Users

- Add the IPSecCerts.der, IPSecKeys.pvk, and IPSecPolicy.spd files to an unzipped image of Cisco Secure VPN Client.
- Post these files as-is to a network drive or web site, or copy to a zip disk

  or

  Zip these files and copy to a floppy disk or CD-ROM.
- Give the files to your end users, along with installation instructions and the password you entered when you exported the certificates and public/private keys.

You are done! When your end users install Cisco Secure VPN Client, it will automatically load their digital certificates, public/private key pairs, and security policies.

Obtaining Documentation

Related Documentation

You can access related Cisco technical documents on the World Wide Web at http://www.cisco.com/univercd/home/home.htm.

Product-specific Documentation

Documentation related specifically to the Cisco Secure VPN Client includes the following publications:

- *Cisco Secure VPN Client Quick Start Guide* at

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvcd.htm

- *Cisco Secure VPN Client Release Notes* at

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvcd.htm

- *Cisco Secure VPN Client Solutions Guide* at

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnsg/index.htm

Cisco IOS Software Documentation

Documentation related to Cisco IOS software includes the following publications:

- *Cisco IOS Release 12.0 Security Configuration Guide* at

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_c/index.htm

- *Cisco IOS Release 12.0 Security Command Reference* at

  http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/secur_r/index.htm

- Cisco Secure PIX 5.1 documentation at

  http://www.cisco.com/univercd/cc/td/doc/product/iaabu/pix/pix_v51/index.htm

World Wide Web

You can access the most current Cisco technical and marketing documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships with most products. The Documentation CD-ROM is updated monthly. Therefore, it is probably more current than printed documentation. The CD-ROM package is available as a single unit or as an annual subscription.

Ordering Documentation

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.

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 may 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.

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to warranty or maintenance contract customers who need technical assistance with a Cisco product that is under warranty or covered by a maintenance contract.

To display the TAC web site that includes links to technical support information and software upgrades and for requesting TAC support, use www.cisco.com/techsupport.

To contact by e-mail, use one of the following:

Language	E-mail Address
English	tac@cisco.com
Hanzi (Chinese)	chinese-tac@cisco.com
Kanji (Japanese)	japan-tac@cisco.com
Hangul (Korean)	korea-tac@cisco.com
Spanish	tac@cisco.com
Thai	thai-tac@cisco.com

In North America, TAC can be reached at 800 553-2447 or 408 526-7209. For other telephone numbers and TAC e-mail addresses worldwide, consult the following web site: http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml.

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 and value your comments.