Release Notes for the Cisco Secure VPN Client Version 1.1

March 23, 2000

Cisco Secure VPN Client (VPN Client) provides client-to-gateway Virtual Private Networking capability on a Windows 95, Windows 98, and Windows NT desktop or laptop computer. The information in this document applies to version 1.1 of the VPN Client.

For information on versions 1.0 and 1.0a features, installation notes, limitations and restrictions, usage notes, and caveats, refer to the following URL:

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

Note If you have a previous version of SafeNet/SoftPK Client or Cisco Secure VPN Client on your machine, you must uninstall this version before you install Cisco Secure VPN Client. For example, you must uninstall VPN Client version 1.0a before you install VPN Client version 1.1. For more information, see the "Installation Notes" section on page 4.

Contents

These release notes contain the following sections:

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

- Obtaining Documentation
- Obtaining Technical Assistance

Introduction

The Cisco Secure VPN Client provides Virtual Private Networking (VPN) capability on a desktop or laptop computer. Based on the latest industry-standard IPSec recommendations, the VPN Client enables secure client-to-gateway communications over TCP/IP networks, including the Internet.

Note Cisco Secure VPN Client is also referenced as SafeNet/Soft-PK version 2.1.2, build 16, in the software. Also, the SafeNet icon appears as the graphical user interface icon in the Windows taskbar. Unless the taskbar is changed, this icon appears in lower right corner of the screen.

The VPN Client gives you the tools you need to use public key encryption for your secure Internet communications. It automatically generates the public/private key pair you need to obtain a digital certificate. It lets you import and maintain digital certificates in its Certificate Manager, and it allows you to import or configure your Secure Connection in its Security Policy Editor.

System Requirements

The following sections list the computer and network requirements. Refer to http://www.cisco.com/go/vpnclient for the latest version of the release notes.

The VPN Client requires the following:

- PC-compatible computer with a Pentium processor
- One of the following operating systems (U.S. English version only):
  - Microsoft Windows 95 (Version 4.00.950 B, 4.00.959 C)
  - Microsoft Windows 98 (98, 98 Second Edition)
  - Microsoft Windows NT Workstation, version 4.0, with Service Pack 4, 5, or 6
- At least 16 MB of RAM for Windows 95 and Windows 98, or 32 MB of RAM for Windows NT Workstation
- Approximately 9 MB available hard disk space
- CD-ROM drive
- Internal/external modem (non-encrypting) or an Ethernet network connection with an NDIS-compliant driver
- Microsoft TCP/IP communications stack and Microsoft dialer (only)

Network Requirements

- Cisco IOS Release 12.1(1)T
- Cisco Secure PIX Firewall version 5.1(1)

New and Changed Information

The sections that follow describe each new feature and each new enhancement in this release. See “Important Notes” for additional information on new features.

New Features

The following features are available in the VPN Client, version 1.1.

Extended Authentication (Xauth)

IETF Extended Authentication or Xauth provides user authentication within the IKE protocol. Xauth prompts the user for authentication material (user name and password) and verifies this information via the use of an AAA server (RADIUS or TACACS+). Authentication occurs between IKE phase 1 and IKE phase 2. If the user successfully authenticates, phase 2 SA is established after which data can be sent securely to the protected network.

Token cards are not supported.

Inverse IP InSight Activator

The IP InSight Activator is a Service Level Management software that has been installed in conjunction with an OEM software manufacturer for measuring performance of remote access VPNs. The software is not fully functional until it receives instructions from a corporate network site to “activate,” and begin sending quality of service data to the network operations center.

The IP InSight Activator is launched at install time, and at all subsequent reboots. Once “activated,” the full IP InSight Client is installed in the directory \<install_directory>\Inverse IP InSight. For more information about the IP InSight Activator, see the readme1st.txt file in the directory \<install_directory>\Cisco\Cisco Secure VPN Client\IP InSight.

RA SCEP

Simple Certificate Enrollment Protocol (SCEP) is a certificate enrollment protocol based on common and well understood PKCS #10/7 standards using HTTP transport methods. SCEP provides a standard way to enroll network devices with a Certification Authority, as well as to lookup and retrieve CRL information from LDAP or HTTP methods. Version 1.1 of the VPN Client now supports the Registration Authority (RA) mode for SCEP enrollment. RA SCEP is currently supported by the Entrust and Microsoft CAs.

Certificate Manager

- Under the My Certificates tab, the Request Certificate dialog box now has the Generate exportable key check box. If you select this check box, you will be able to export your private key with your personal certificate. In previous versions, this was the default. Now you must select this check box when you make your request, or you will not have the option to export your private key with your personal certificate.
- Under the Certificate Requests tab, when you view a certificate request, you will see a SHA1 fingerprint and an MD5 fingerprint. This allows you to verify with your CA over the phone that the request has not been tampered with.

- Under the My Certificates tab or the CA Certificates tab, when you view a digital certificate, you can now see Key Usage if it is defined for that certificate. The following key usages may appear here: CRL Signing, Data Encipherment, Digital Signature, Key Agreement, Key Certificate Signing, Key Encipherment, and Non Repudiation.
- Certificate chains longer than 2 are now supported.

Feature Enhancements/Improvements

The following are feature enhancements or improvements available in the VPN Client, version 1.1:

Security Policy Editor

- Under My Identity, Local Network Interface has been renamed Internet Interface.
- Under Authentication (Phase 1) and Key Exchange (Phase 2), the new default setting for the encryption algorithm is DES, and the new default setting for the hash algorithm is SHA-1.
- Under Key Exchange (Phase 2), there are no longer two separate SA Life list boxes. These have been combined into one SA Life list box that applies to both ESP and AH, whichever is selected.

Installation Notes

Note If you are installing on a Windows NT system, log on through the administrator account, before installing the VPN Client.

Note If you are upgrading from a previous version of SafeNet/SoftPK Client or Cisco Secure VPN Client, uninstall the old version, then reboot, then install the new version. If the old version is not uninstalled, two images and two identical icons in the system taskbar are created and the new version will be corrupted.

To install the VPN Client, perform the following steps:

Step 1 Close all other programs before continuing.

Step 2 If you are upgrading from a previous version of SafeNet/SoftPK Client or Cisco Secure VPN Client, uninstall the old version, then reboot, then install the new version. When you uninstall a previous version, you may keep any existing key pairs, personal certificates, and security policies.

Step 3 Insert the Cisco Secure VPN Client CD-ROM. The installation program should start automatically. If it does not, perform the following:

a. Click **Start**>**Run**.

b. Type **`d:\setup.exe`** (`d` designates your CD-ROM drive, which could be different depending on your computer's setup).

Step 4 When the Installation Wizard starts, follow the instructions on your screen.

Step 5 When the setup completes, select **Yes, I want to restart my computer now**. Remove the CD-ROM, and click **Finish**. Your computer will automatically restart.

The SafeNet icon appears in the status area of your Windows taskbar, which is usually located in the lower right corner of your screen.

Step 6 Once you have successfully installed VPN Client, you need either a pre-shared key or a digital certificate and a Secure Connection to secure communications. Look for detailed instructions in your *Cisco Secure VPN Client Version 1.1 Quick Start Guide* or help file. To access the help file, right-click the SafeNet icon on the taskbar and click **Help**.

Running Cisco Secure VPN Client

The VPN Client starts automatically each time your computer starts, and runs transparently on your computer.

The SafeNet icon changes color and image as you begin and end communications sessions:

- Green indicates your computer is transmitting secure communications.
- Red indicates it is transmitting unsecure communications (both red and green can appear at the same time).
- A key symbol indicates that your computer is ready to transmit secure communications.

For more information, review the help file, which you can view by right-clicking the SafeNet icon on the taskbar, or from the Help menu in the Security Policy Editor or Certificate Manager.

Note Before calling customer support, display the View Log by right-clicking the SafeNet icon on the taskbar and clicking **Log Viewer**.

Temporarily Deactivating the Cisco Secure VPN Client

You can temporarily deactivate the client by right-clicking the SafeNet icon on the taskbar and clicking **Deactivate Security Policy**. When you are ready to restart the client, click **Activate Security Policy** on this same menu.

Uninstalling Cisco Secure VPN Client

Note You could be violating your organization's Secure Connection by removing this software from your hard drive. Check with your network administrator before continuing.

To uninstall VPN Client:

Step 1 Click **Start**>**Settings**>**Control Panel**.

Step 2 Double-click **Add/Remove Programs**. The Add/Remove Programs Properties window appears.

Step 3 Click the **Install/Uninstall** tab.

Step 4 Click **Cisco Secure VPN Client** from the list.

Step 5 Click **Add/Remove**.

Step 6 You are prompted with the following:

```
Are you sure you want to completely remove ‘Cisco Secure VPN
Client’ and all of its components?
```

Click **Yes**. You will still be prompted to save or delete your certificates and key pairs.

Step 7 The uninstall starts, and you are prompted with the following:

```
Would you like to delete Security Policy Personal Certificates
and Private/Public Keys?
```

If you plan to reinstall this product, click **No**; otherwise, click **Yes**.

Step 8 After the uninstallation completes, if any files were in use, you are prompted with a reminder that you should restart your computer to remove files in use during the uninstallation. Click **OK** at this prompt to acknowledge this reminder.

Step 9 Restart your computer now by clicking **Start**>**Shutdown**.

Limitations and Restrictions

The following restrictions apply to the VPN Client, version 1.1:

- Any previous version of the Cisco Secure VPN Client or SafeNet/Soft-PK Client must be removed from the Windows system before installing the VPN Client.
- The VPN Client does not support the option to specify on the VPN Client the IP address of the VPN Client while also enabling IKE Mode Configuration on the VPN security gateway. When enabling the IKE Mode Configuration feature within the VPN security gateway, under Options, do not select the Allow to Specify Internal Network Address option in the Global Policy Settings dialog box within the VPN Client.

Important Notes

This section provides information about using VPN Client, version 1.1.

3Com Smart Agent Software

The VPN Client will not install properly if 3Com’s Smart Agent software is loaded on the machine before installing VPN Client.

Cisco recommends that you install the VPN Client before installing 3Com’s Smart Agent software.

AtGuard PC Firewall

The VPN Client is incompatible with AtGuard PC firewall on Windows 98 SE. Loading the VPN Client on a Windows 98 SE machine with AtGuard PC firewall causes the machine to no longer pass secure or clear data.

AT&T Dial-In

The AT&T Global Network Dialer software and the VPN Client when installed on Windows 98 are incompatible. With both are installed on Windows 98, the AT&T Global Network Dialer software cannot dial to Internet.

When the AT&T Global Network Dialer software installs itself, it places a shortcut on your desktop. This shortcut is linked to a program called `connect.exe`. Do not run this program. Instead use the Dial-Up Networking program. To get to this program, click the My Computer icon on your desktop, then select **Dial-Up Networking**. From the Dial-Up Networking window, dial up your connection.

Certificate Enrollment

When using digital certificates, use a unique subject name for each VPN Client. Otherwise, when terminating multiple connections, the security gateway will not be able to determine which public key to use during authentication since the public key is chosen based on the VPN Client's subject name.You are prompted to enter a subject name after choosing the **Request Certificate** button from the **My Certificates** tab in the **Certificate Manager** window.

IPSec Protocols

The VPN Client lets you specify various combinations of IPSec protocols on the menu at **Network Security Policy**>*connection_name*>**Security Policy**>**Key Exchange (Phase 2)**>**Proposal**.

PIX Firewall and Cisco IOS software support all VPN Client IPSec protocols with these exceptions:

- PIX Firewall and Cisco IOS software do not support the DES-MAC hash algorithm.
- PIX Firewall and Cisco IOS software do not support the DH5.
- PIX Firewall and Cisco IOS software can use both AH (Authentication Header) and ESP (Encapsulated Security Protocol) in a single Secure Connection, but the VPN Client can use only one of the two per Secure Connection.

Microsoft CA Server

If you see the error message “integrity check failed” when submitting your certificate request, check your version of the MSCEP.DLL. The version must be greater than 5.131.2195.1.

Microsoft Dial-Up Networking

Before upgrading Microsoft Dial-Up Networking (DUN), uninstall the Cisco Secure VPN Client. Once DUN is installed and configured, reinstall the client. When you uninstall the VPN Client, you can choose not to delete Security Policy Personal Certificates and Private/Public Keys. We require MS DUN version 1.3 or later.

MSN’s Connection Manager

The VPN Client is incompatible with Microsoft's Connection Manager.

The auto setup part of Microsoft's MSN package is incompatible with intermediate drivers between the dialup adapter and TCP/IP. The result is that connection manager attempts to re-add TCP/IP ad infinitum, until the max instance value is reached.

As a workaround, Cisco recommends that MSN users configure the Dialup adapter and TCP/IP and Internet Explorer manually. For example, if the adapter and TCP/IP are loaded before installing MSN, the Microsoft Connection Manager detects that the dial-up adapter is already installed and continues with the MSN installation. The VPN Client can be loaded before or after MSN, if the dial-up adapter and TCP/IP are installed manually.

MSN’s Internet Connection

The VPN Client and Microsoft's Internet Connection Sharing (ICS) for Windows 98 Second Edition are incompatible. If you attempt to install the VPN Client over ICS or vice versa, the VPN Client does not install or is automatically uninstalled. To check for ICS, look for the following key in the Windows registry:

HKEY_LOCAL_MACHINE\Enum\Network\ICSHAREP

If this key is present, uninstall the ICS and try installing the VPN Client again.

Providing Users a Standard Secure Connection

You can provide users a standardized Secure Connection by creating it with the values you determine, and then exporting it by clicking **File**>**Export Security Policy**. When you are prompted to protect the exported Secure Connection by making it non-editable, click **Yes**. When users open the Secure Connection, the Connection Security information displays the message that it is Secure. Users can view the parameters, but they cannot change them.

Note Before importing an non-editable Secure Connection, make sure you have at least one editable Secure Connection on your system. If you do not have an editable Secure Connection available to you and if you want to change the locked Secure Connection, you must reinstall.

Remote Party Identity and Addressing

The Remote Party Identity and Addressing menu appears on the Connection menu after you start a new Network Security Policy.

The following ID Type values are supported as follows:

- IP Address—supported by both PIX Firewall and Cisco IOS software
- Domain Name—supported by both PIX Firewall and Cisco IOS software
- E-Mail Address—not supported by either PIX Firewall or Cisco IOS software
- IP Subnet—supported by both PIX Firewall and Cisco IOS software

- IP Address Range—not supported by either PIX Firewall or Cisco IOS software
- Distinguished Name—not supported by either PIX Firewall or Cisco IOS software

Secure Connections

Before you configure a Secure Connection, you must already have established a connection and configured the preliminary settings through the **Options**>**Secure**>**All Connections or Specified Connections** options.

The purpose of configuring a Secure Connection is to create a security association (SA) for each connection through IKE negotiations.

There are two phases to every IKE negotiation, which you must also configure:

- **Phase 1 - Authentication**—During Phase 1, individuals reveal their identities and negotiate how they will secure Phase 2 communications. Phase 1 can be one of two types:
  - Main Mode. This mode protects identities, which are not revealed until secure communications have been established.
  - Aggressive Mode. This mode speeds the negotiation; identities are revealed before secure communications have been established, reducing the number of Phase 1 steps. This is a less secure option as a result of the accelerated negotiation.

  Note When creating multiple IPSec SAs to the same Secure Gateway, only one IKE SA will be used. This means that one IKE SA is established to protect multiple IPSec SAs. When multiple Secure Connections are defined to the same secure gateway, their Authentication (Phase 1) proposals must be identical.

  Specifying different Phase 1 proposals for multiple Secure Connections that use a single security gateway causes unpredictable results. If you create multiple Secure Connections to the same security gateway, use identical Phase 1 proposals.

- **Phase 2 - Key Exchange**—During Phase 2, also known as Quick Mode, individuals negotiate the encryption and message authentication algorithms and develop the necessary shared keys to be used for secure communications. Phase 2 communications are secured as negotiated during Phase 1.

Note Toggling between **Secure, Block**, and **Non-secure** on a Secure Connection may cause a subnet defined in **Remote Party Identity and Addressing** to change the ID type to **IP Address**. The user will need to redefine the ID type.

Security Association Lifetimes

Note Cisco recommends that when configuring SA lifetimes, use seconds or apply the default value of **Unspecified** (28,800 seconds).

Authentication (Phase 1)

The default Internet Key Exchange (IKE) lifetime on the VPN gateway is 24 hours (86,400 seconds), the client has a default of 8 hours (28,800 seconds), and the PIX Firewall has a default of 24 hours.

The client may offer any value to the VPN gateway, with the lower of the two lifetimes used.

Key Exchange (Phase 2)

On the menu at **Network Security Policy**>*connection_name*>**Security Policy**>**Key Exchange (Phase 2)**>**Proposal**, you can set the IPSec SA Life (lifetime) value to either **Seconds** or **Kbytes** (kilobytes). When specifying a lifetime in seconds, the peers, whether client and Cisco router or client and PIX Firewall, will agree to use the smaller of the values proposed by each peer.

By default, the router uses 1 hour (3,600 seconds), the VPN Client uses 8 hours (28,800 seconds), and the PIX Firewall uses 8 hours for the IPSec SA lifetime. We recommend using the default values for optimal stability.

Signal 9 ConSeal PC Firewall

The VPN Client is incompatible with Signal 9 ConSeal PC Firewall on Windows 98. Loading the VPN Client on a machine with Signal 9 ConSeal PC Firewall causes the machine to no longer pass secure or clear data.

VeriSign CA

When enrolling a client with the VeriSign CA service, the domain name field of the online request must contain the FQDN (fully qualified domain name) of the device.

View Log

You can display the view log by right-clicking the SafeNet icon on the taskbar and clicking **Log Viewer**.

Windows NT Domain Authentication

A delay may occur between the time the Windows network login prompt appears and the actual establishment of the IPSec tunnel. This delay may cause the login attempt to time out because a server is not available. If this occurs, cancel the first attempt and retry. Use the event log on the VPN Client during this process to view login status.

Windows NT Plug and Play Drivers

Windows NT does not support Plug and Play via a manufacturer’s custom utility, and the VPN Client is incompatible with these custom, non-standard, non-NDIS-compliant utilities.

As a workaround in the case of the laptop utilities, disable the manufacturer’s custom utility and obtain the latest NIC driver from the vendor. (Ensure that you do not obtain the special pre-packaged NIC driver that the laptop vendor supplies with the utility).

Caveats

This section covers the open and resolved caveats within the VPN Client, version 1.1.

Open Caveats

The open caveats described in this section provide important information that you need to run the VPN Client. Table 1 lists the caveats for version 1.1.

If you have an account with Cisco Connection Online (CCO), you can use the Bug Toolkit to determine the status of open caveats:

1. Access CCO at http://www.cisco.com.
2. Click **Login** on the upper toolbar. When prompted, enter your CCO username and password.
3. Go to the Bug Toolkit on CCO at **Service & Support**>**Online Technical Support**>**Software Bug Toolkit**>**Search for Bug by ID Number**, or at http://www.cisco.com/kobayashi/bugs/bugs.html.
4. Enter the bug ID number and click **Search** to view the current status.

Table 1 lists the open caveats for version 1.1:

Table 1 Open Caveats for Version 1.1

DDTS ID	Description
Certificate Issues	
CSCdm69390	The Security Policy Editor must be closed and reopened before changes made in the Certificate Manager are visible to the Secure Connection.
CSCdm69392	For remote identity or a Security Gateway when using certificates, the identity type has to be **Domain Name** and the identity has to be specified as **FQDN**. Also, the IP address has to be specified because the FQDN is not resolvable on the VPN Client computer.
CSCdm69393	The VPN Client has a fixed CRL (Certificate Revocation List) download period of 4 hours. As a result, if the CRL has expired, the client will not be able to identify the validity of the remote peer's certificate. In this case, the client will not establish an IKE SA until the CRL is updated. As a workaround, we recommend setting the CA's CRL lifetime to 24 hours. This reduces the likelihood of the client acquiring a CRL with an imminent expiration.
CSCdr05403	Unable to generate digital certificate requests when the & character is used within the Name, Department, or Company fields. As a workaround, Cisco recommends not using the & character in the certificate request.

Table 1 Open Caveats for Version 1.1 (continued)

DDTS ID	Description
CSCdr05418	Importing a certificate chain overwrites the CA properties that are within the cacert.cser file. If the personal certificate with the CA chain file is imported after the SCEP properties have been configured, the SCEP CA properties (CA domain and On-Line certificate server information) are lost. This problem can also occur during a VPN Client install. If a personal certificate with CA chain file and a “Cacert.cser” file are bundled with the initial install, the SCEP CA properties that are included with the “Cacert.cser” file are lost. The root cause of this problem is that the personal certificate with the CA chain does not actually contain the SCEP CA properties information. To avoid overwriting the CA certificate settings while importing the certificate chain, Cisco recommends the user answers *no* to adding the CA certificate. During install, do not include the CA chain with the personal certificate.
Miscellaneous	
CSCdm55397	Uninstall any previous version of the SafeNet/SoftPK Client or Cisco Secure VPN Client before installing a new version of the VPN Client.
CSCdm88654	The VPN Client is not interoperable with VeriSign CRLs.
CSCdm89035	Before adding or removing any network adapters from the Network Control Panel, uninstall the VPN Client, and reboot the computer. After the adapters are configured appropriately, reinstall the client. If this procedure is not followed you may experience system instability upon rebooting after adapters have been added or removed. You can recover by starting your Windows system in Safe Mode, uninstalling the client, rebooting, and then reinstalling the client.
CSCdp79684	Exporting a policy as protected does not make the new configuration non-editable. Users can still change any parameter under My Identity. This will allow a single policy to be exported and distributed to multiple clients.
CSCdp86758	In rare circumstances, uninstalling the VPN Client on a Windows NT system may take up to 15 minutes to complete. If you end the uninstall process before it completes on its own, reinstall the same VPN Client version and uninstall again.
CSCdr03653	When using a pre-shared key and the Aggressive Mode of IKE Phase 1, specifying the ID type of “Domain Name” within the My Identity window fails. As a workaround, Cisco recommends specifying either **Email Address** or **IP Address** for ID type.
CSCdr05380	For secure domain logon, Cisco recommends you wait 10 seconds after a failed domain login attempt.
CSCdr06345	The VPN Client does not always prompt the user to reboot after an uninstall. As a precaution, the user should always reboot after uninstallation.
CSCdr06441	When using Windows 95, the VPN Client will not function after coming out of the suspend mode. If this occurs, reboot your system. To ensure it does not occur again, disable the suspend mode.

Table 1 Open Caveats for Version 1.1 (continued)

DDTS ID	Description
CSCdr08637	Fingerprints are not supported for manual (file-based) certificate requests or for CAs manually imported from a file.
CSCdr30330	The client may truncate part of a new pin message displayed to the user when using Xauth with a token card. The amount of truncation will depend on the token authentication server used.

Resolved Caveats

Table 2 lists resolved caveats for version 1.1:

Table 2 Resolved Caveats for Version 1.1

DDTS ID	Description
CSCdm50577	The interoperability problems with per port support within IPSec are fixed.
CSCdm60716	Security Policy Editor/Certificate Manager: On Windows NT workstations, the VPN Client now operates with non-Administrator users.
CSCdm69381	If the VPN Client is configured to send less than the Cisco IOS software default for IKE (86,400 seconds—24 hours), the lifetime proposed by the VPN Client will be used.
CSCdm69396	On Windows NT Service Pack 4, when adding a new CA certificate (online through SCEP or importing from a file) a confirmation dialog displays.
CSCdm80701	Configuring the client for TCP traffic will only allow TCP traffic.
CSCdp10777	For security purposes, pre-shared keys are now starred out during entry and encrypted in the registry. Importing of a previous policy or upgrading from a previous policy will automatically encrypt the pre-shared key.
CSCdp19890	The Windows NT domain logon no longer fails when the VPN Client is assigned an internal IP address with either IKE Mode Config or static assignment.
CSCdp22155	The VPN Client now functions through a Network Address Translation device, such as a firewall.
CSCdp46826	The VPN Client co-exists with Token Ring cards and allows IPSEC sessions over dial-up connections. IPSEC sessions over Token Ring cards are not supported.

Related Documentation

Use this document in conjunction with the following related documents, which are available on CCO and the Documentation CD-ROM:

Note Refer to the CCO online version of these release notes for the most current information.

- *Cisco Secure VPN Client Version 1.1 Quick Start Guide:*

  On CCO: http://www.cisco.com/univercd/cc/td/doc/product/iaabu/csvpnc/csvpnqs/vcq11.htm or **Technical Documents**>**Documentation Home Page**>**Internet Service Unit**>**Cisco Secure VPN Client**>**Cisco Secure VPN Client Quick Start Guides**>**Cisco Secure VPN Client - Quick Start Guide for Version 1.1**

On the Documentation CD-ROM: **Cisco Product Documentation**>**Internet Service Unit**>**Cisco Secure VPN Client**>**Cisco Secure VPN Client Quick Start Guides**>**Cisco Secure VPN Client - Quick Start Guide for Version 1.1**

- *Cisco Secure VPN Client Solutions Guide:*

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

  or **Technical Documents**>**Documentation Home Page**>**Internet Service Unit**>**Cisco Secure VPN Client**>**Cisco Secure VPN Client Solutions Guide**

  On the Documentation CD-ROM: **Cisco Product Documentation**>**Internet Service Unit**>**Cisco Secure VPN Client**>**Cisco Secure VPN Client Solutions Guide**
- Cisco IOS Release 12.1 software documentation:

  On CCO: http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/index.htm

  or **Technical Documents**>**Documentation Home Page**>**Cisco IOS Software Configuration**> **Cisco IOS Release 12.1**

  On the Documentation CD-ROM: **Cisco Product Documentation**>**Cisco IOS Software Configuration**>**Cisco IOS Release 12.1**
- Cisco Secure PIX Firewall Version 5.1 documentation:

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

  or **Technical Documents**>**Documentation Home Page**>**Internet Service Unit**>**Cisco Secure PIX Firewall**>**PIX Firewall Version 5.1**

  On the Documentation CD-ROM: **Cisco Product Documentation**>**Internet Service Unit**>**Cisco Secure PIX Firewall**>**PIX Firewall Version 5.1**

Obtaining Documentation

World Wide Web

You can access the most current Cisco 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 your product. 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.

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

Language	E-mail Address
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.

This document is to be used in conjunction with the documents listed in the “Related Documentation” section.