Text Part Number: 78-6929-03

Release Notes for the Cisco Secure VPN Client Versions 1.0/1.0a

December 1999

Cisco Secure 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 versions 1.0 and 1.0a of the Cisco Secure VPN Client.

The only caveat resolved in version 1.0a is CSCdp19890.

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 Cisco Secure VPN Client version 1.0 before you install Cisco Secure VPN Client version 1.0a. For more information, see the "Installation Notes" section on page 4.

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

Contents

These release notes contain the following sections:

Introduction

Cisco Secure VPN Client provides Virtual Private Networking (VPN) capability on a desktop or laptop computer. Based on the latest industry-standard IPSec recommendations, Cisco Secure 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 2.0 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.

Cisco Secure 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.

Cisco Secure VPN Client requires the following:

- PC-compatible computer with a Pentium processor
- One of the following operating systems:
  - Microsoft Windows 95
  - Microsoft Windows 98
  - Microsoft Windows NT version 4.0 with Service Pack 3, 4, or 5
- At least 16 MB of RAM for Windows 95 and Windows 98, or 32 MB of RAM for Windows NT 4.0
- 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

- For 7*xxx* series routers, use Cisco IOS Release 12.0(5)XE
- For other VPN-enabled routers, use Cisco IOS Release 12.0(5)T1 (mode config is not supported in this Cisco IOS software version)
- Cisco Secure PIX Firewall version 5.0

Installation Notes

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

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 and certificates.

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 Cisco Secure 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 Quick Start Guide* or help file. To access the help file, right-click the SafeNet icon on the taskbar and select **Help**.

Running Cisco Secure VPN Client

Cisco Secure 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 means it is transmitting unsecure communications (both red and green can appear at the same time).
- A key symbol means 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 Cisco Secure 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 If prompted to restart your computer, click **OK**.

Step 10 Restart your computer now by clicking **Start**>**Shutdown**.

Limitations and Restrictions

The following restrictions apply to both version 1.0 and 1.0a:

- Any previous version of the Cisco Secure VPN Client or SafeNet/Soft-PK Client must be removed from the Windows system before installing the Cisco Secure VPN Client.
- When using the online, CEP-based enrollment method for the client to any Certification Authority (CA) server, the client and CA fingerprint are not displayed. These fingerprints must be viewed and verified during the CEP process. Failure to do this renders the certificate enrollment vulnerable to a "man-in-the-middle" attack. For this reason, CEP enrollment should occur only on a trusted network.
- Cisco Secure VPN Client does not support manual keys.
- Cisco Secure PIX Firewall and Cisco IOS software do not support Port selection in both version 1.0 and 1.0a. Port selection is set in the Security Policy Editor in the **Network Security Policy**>*connection_name*>**Remote Party Identity and Addressing**>**Port** or from **Network Security Policy**>*connection_name*>**My Identity**>**Port**.

Important Notes

This section provides information about using Cisco Secure VPN Client, versions 1.0. and 1.0a.

Entrust CA

The Entrust CA is supported through the file method. After you have installed the Cisco Secure VPN Client, you can view the **Create a certificate request file** online help topic for information about the file method. You can access online help from the Security Policy Editor, Certificate Manager, or by right-clicking the SafeNet taskbar icon. When the online help appears, click the **Contents** tab. The **Create a certificate request file** help topic is located in the **Working with Digital Certificates**>**Requesting Digital Certificates from CAs**>**Manual Enrollment** topic folder.

Cisco Secure VPN Client does not support the use of CEP with the Entrust CA.

Equant Dial Service

Installing the client causes Equant dial service to fail if the Inverse IP Insight tool is also present. The Equant Dial Manager software must be installed after the client has been installed.

When removing the Equant Dialer, remove the Inverse IP Insight application, and then install the Cisco Secure VPN Client.

IPSec Protocols

Cisco Secure 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 Cisco Secure 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 can use both AH (Authentication Header) and ESP (Encapsulated Security Protocol) in a single Secure Connection, but the Cisco Secure VPN Client can use only one of the two per Secure Connection.

Internal Network Address

You can specify an internal network address on the Security Policy Editor's My Identity menu by clicking **Options**>**Global Policy Settings**. In the Global Policy Settings dialog box, select the **Allow to Specify Internal Network Address** check box.

The Internal Network IP Address field then appears in the My Identity menu to the right of the ID Type field.

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 Cisco Secure VPN Client, you can choose not to delete Security Policy Personal Certificates and Private/Public Keys. We recommend MS-DUN version 1.3 or later.

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

Security Association Lifetimes

Note Cisco Secure VPN Client maintains only one pair of SAs for a given peer. Ideally, Cisco Secure VPN Client should always be the initiator when re-keying. If this does not happen, connectivity between the client and gateway may be disrupted temporarily until the new SA is used. This disruption may cause some application sessions to timeout. Once the new SA is used, connectivity is restored and the user should restart the application. We recommend 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 Cisco IOS router 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 must offer less than or the same lifetime value as the router. The smaller of the two lifetimes is negotiated. However, if the router is configured to use the default, this is the value applied, regardless of the lifetime proposed by the client.

The client may offer any value to the PIX Firewall, 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 Cisco Secure 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.

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 Cisco Secure VPN Client does not support manual keys.

Note When defining a Quick Mode Secure Connection for IPSec, PIX Firewall and Cisco IOS software can use both AH and ESP in a single Secure Connection, but the Cisco Secure VPN Client can use only one of the two per Secure Connection.

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**.

Caveats

Open Caveats for Version 1.0

The open caveats described in this section provide important information that you need to run the Cisco Secure VPN Client. Table 1 lists the caveats for version 1.0. These open caveats also apply to version 1.0a.

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 1.0:

Table 1 Open Caveats

DDTS ID	Description
Issues with Security Association Lifetimes	
CSCdm69419 and CSCdm80566	Cisco Secure VPN Client maintains only one pair of SAs for a given peer. Ideally, Cisco Secure VPN Client should always be the initiator when re-keying. If this does not happen, connectivity between the client and gateway may be disrupted temporarily until the new SA is used. This disruption may cause some application sessions to timeout. Once the new SA is used, connectivity is restored and the user should restart the application. We recommend that when configuring SA lifetimes, use seconds or apply the default value of **Unspecified** (28,800 seconds).
CSCdm69381	If the client is configured to send less than the Cisco IOS software default for IKE (86,400 seconds—24 hours), IKE will succeed but the lifetime set at the router will be the Cisco IOS software default, not the value proposed by the client. A workaround is to set the Cisco IOS software IKE lifetime to be the same as that of the client.
Certificate Issues	
CSCdm69396	On the Windows NT 4.0 Service Pack 4, when adding a new CA certificate (online through CEP or importing from a file) no confirmation dialog is displayed.
CSCdm69393	The Cisco Secure 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.
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 Cisco Secure VPN Client computer.

Table 1 Open Caveats (continued)

DDTS ID	Description
CSCdm69390	The Security Policy Editor must be closed and reopened before changes made in the Certificate Manager are visible to the Secure Connection.
Miscellaneous	
CSCdm81468	You may experience delays when setting up multiple secure connections from a single client to the same Cisco IOS software gateway.
CSCdm89035	Before adding or removing any network adapters from the Network Control Panel, uninstall the Cisco Secure 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.
CSCdm88523	The Security Policy Editor dialog may continuously loop under the following conditions: • If the ID Type for a Connection Entry just above "Other Connections" is not IP Address, and • You delete this Connection Entry with the "Other Connections" entry highlighted, and • You click **Save** while "Other Connections" is still highlighted. A dialog box then appears and displays the following: `SPDEDIT: The parameter value is invalid for the address type selected.` If you click OK, the dialog box then continuously reappears. The workaround is to delete the connection entry, move the highlight away from the "Other Connections" Secure Connection, and save the changes.

Table 1 Open Caveats (continued)

DDTS ID	Description
CSCdm80701	Configuring the client for TCP traffic only also allows all UDP traffic if the gateway proposes the UDP-based Secure Connection. Generally, traffic is initiated from the client side, so this behavior is rare. **Note** This scenario does not apply to the PIX Firewall.
CSCdm80643	Installing the client causes Equant dial service to fail if the Inverse IP Insight tool is also present. The Equant Dial Manager software must be installed after the client has been installed. When removing the Equant Dialer, remove the Inverse IP Insight application, and then install the Cisco Secure VPN Client.
CSCdm69425	Toggling between **Secure**, **Block**, and **Non-secure** on a Secure Connection may cause a subnet defined as **Remote Party Identity ID** to change to **IPAddress ID**. The user will need to redefine the ID type.
CSCdm68679	When using mode config with Cisco Secure PIX Firewall and Cisco IOS software, more than one IP address may be used by a client, consequently, the error starting with "Non-Secure Connection" may appear in the View Log. This does not affect the traffic in any way and can be ignored.
CSCdm60716	Client and Windows NT privileges—The client must be installed and started from the Windows NT administrator login.
CSCdm55397	Uninstall any previous version of SafeNet/Soft-PK Client or Cisco Secure VPN Client before installing a new version of Cisco Secure VPN Client.

Open Caveats for Version 1.0a

There are no new open caveats in version 1.0a.

Resolved Caveats for Version 1.0

There are no new resolved caveats in version 1.0.

Resolved Caveats for Version 1.0a

Caveat CSCdp19890 was resolved in version 1.0a. When you assign an internal IP address via either mode config or static configuration, attempts to log in to a Windows NT network may fail. The fix in CSCdp19890 uses the client's internal IP address as the source address in the NetBIOS payload, which lets the Windows NT Server successfully respond to the client.

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 Cisco Secure VPN Client during this process to view login status.

Related Documentation

Use this document in conjuction with the *Cisco Secure VPN Client Quick Start Guide* included with the CD-ROM and available on CCO, and also with the online help included with the software. Also use this document in conjunction with the CCO online version of the *Cisco Secure VPN Client Solutions Guide* available at the following Cisco Secure VPN Client documentation site:

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

Refer to the CCO online version of these release notes at the Cisco Secure VPN Client documentation site for the most current information.

Cisco Connection Online

Cisco Connection Online (CCO) is Cisco Systems' primary, real-time support channel. Maintenance customers and partners can self-register on CCO to obtain additional information and services.

Available 24 hours a day, 7 days a week, CCO provides a wealth of standard and value-added services to Cisco's customers and business partners. CCO services include product information, product documentation, software updates, release notes, technical tips, the Bug Navigator, configuration notes, brochures, descriptions of service offerings, and download access to public and authorized files.

CCO serves a wide variety of users through two interfaces that are updated and enhanced simultaneously: a character-based version and a multimedia version that resides on the World Wide Web (WWW). The character-based CCO supports Zmodem, Kermit,

Xmodem, FTP, and Internet e-mail, and it is excellent for quick access to information over lower bandwidths. The WWW version of CCO provides richly formatted documents with photographs, figures, graphics, and video, as well as hyperlinks to related information.

You can access CCO in the following ways:

- WWW: http://www.cisco.com
- WWW: http://www-europe.cisco.com
- WWW: http://www-china.cisco.com
- Telnet: cco.cisco.com
- Modem: From North America, 408 526-8070; from Europe, 33 1 64 46 40 82. Use the following terminal settings: VT100 emulation; databits: 8; parity: none; stop bits: 1; and connection rates up to 28.8 kbps.

For a copy of CCO's Frequently Asked Questions (FAQ), contact cco-help@cisco.com. For additional information, contact cco-team@cisco.com.

Note If you are a network administrator and need personal technical assistance with a Cisco product that is under warranty or covered by a maintenance contract, contact Cisco's Technical Assistance Center (TAC) at 800 553-2447, 408 526-7209, or tac@cisco.com. To obtain general information about Cisco Systems, Cisco products, or upgrades, contact 800 553-6387, 408 526-7208, or cs-rep@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, a member of the Cisco Connection Family, is updated monthly. Therefore, it might be more current than printed documentation. To order additional copies of the Documentation CD-ROM, contact your local sales representative or call customer service. The CD-ROM package is available as a single package or as an annual subscription. You can also access Cisco documentation on the World Wide Web at http://www.cisco.com, http://www-china.cisco.com, or http://www-europe.cisco.com.

If you are reading Cisco product documentation on the World Wide Web, you can submit comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco. We appreciate your comments

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