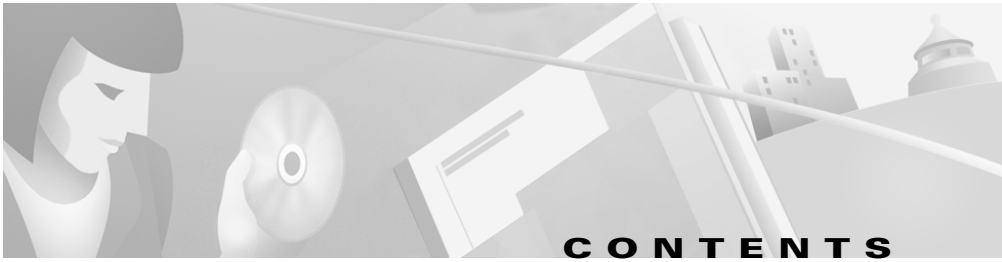
Cisco VPN Client User Guide for Linux

Software Version 3.0.x
August 2001

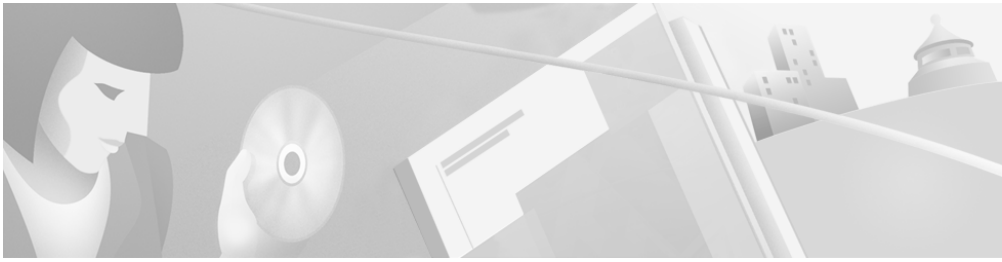
Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-1246-01

Cisco VPN Client User Guide for Linux



CONTENTS



About This Guide

This guide provides users and administrators with information about the Cisco VPN Client software for the Linux for Intel operating system.

Contents

This guide contains the following chapters:

- Chapter 1, “Introduction to the VPN Client.” This chapter provides a brief introduction to the VPN client software.
- Chapter 2, “Installing the VPN Client for Linux.” This chapter describes how to install the VPN client software on your workstation.
- Chapter 3, “User Profiles.” This chapter describes how to set up user profiles.
- Chapter 4, “Using the Command Line Interface.” This chapter describes the command line interface and lists the commands and their descriptions.
- Chapter 5, “Managing Digital Certificates.” This chapter describes how to manage your digital certificate stores.
- Chapter 6, “Preconfiguring the VPN Client for Remote Users.” This chapter describes how administrators can preconfigure the VPN client for remote users.
- Index

Related Documentation

The following is a list of manuals and other documentation related to the VPN client for Linux.

- *Cisco VPN Client Administration Guide*
- *Cisco VPN 3000 Concentrator Series Getting Started*
- *Cisco VPN 3000 Concentrator Series User Guide*
- *Cisco VPN 5000 Concentrator Software Configuration Guide*
- *Cisco VPN 5000 Concentrator Series Command Reference Guide*

Documentation Conventions

The following typographic conventions are used in this manual.

Data Formats

When you configure the VPN client, enter data in these formats unless the instructions indicate otherwise.

- IP Address

  IP addresses use standard 4-byte dotted decimal notation. For example, 192.168.12.34. You can omit leading zeros in a byte position.

- Hostnames

  Hostnames use legitimate network host or end-system name notation; for example, `VPN01`. Spaces are not allowed. A hostname must uniquely identify a specific system on a network. A hostname can be up to 255 characters in length.

- User names and Passwords

  Text strings for user names and passwords use alphanumeric characters in both upper- and lower-case. Most text strings are case sensitive. For example, `simon` and `Simon` would represent two different user names. The maximum length of user names and passwords is generally 32 characters, unless specified otherwise.

Obtaining Documentation

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

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.

Introduction to the VPN Client

The Cisco VPN Client connects a remote user to a corporate network.

The user connects to a local Internet service provider (ISP), then to the VPN device Internet IP address. The VPN client encrypts the data and encapsulates it into a routable IPSec packet, creating a secure tunnel between the remote user and the corporate network.

The corporate server authenticates the user, decrypts and authenticates the IPSec packet, and translates the source address in the packets to an address recognized on the corporate network. This address is used for all traffic sent from the corporate network to the remote user for the duration of the connection.

Features

The VPN client distinguishes between tunneled and nontunneled traffic and, depending on your server configuration, allows simultaneous access to the corporate network and to Internet resources.

The VPN client communicates over PPP links, including dialup and ISDN, and over Internet-attached Ethernet connections, including DSL and cable modem.

Table 1-1 lists the VPN client features.

Table 1-1 VPN Client Features

Feature	Description
Operating systems	• Red Hat 6.2 Linux (Intel), or compatible distribution, using kernel Version 2.2.12 or later
Connection types	• PPP, including dialup and ISDN • Ethernet, including DSL and cable modem
Protocol	IP
Tunnel protocol	IPSec
User authentication	• RADIUS • RSA SecurID • NT Domain • VPN server internal user list • PKI digital certificates

Installing the VPN Client for Linux

This chapter describes how to install the VPN client for Linux. You should be familiar with Linux and software installation on Linux before you perform this procedure.

The VPN client for Linux consists of a driver, which is a loadable module, and a set of commands accessible through your shell, which is used to access the applications.

The commands and some parts of the driver are distributed in binary form only.

Contents

This chapter contains the following sections:

System Requirements

The VPN client for Linux supports Red Hat Version 6.2 Linux (Intel), or compatible libraries with glibc Version 2.1.1-6 or later, using kernel Versions 2.2.12 or later.

Unpacking the VPN Client Files

The VPN client for Linux is shipped as a compressed tar file.

To unpack the files

Step 1 Download the packed files (from either your internal network or the Cisco website) to a directory of your choice.

Step 2 Copy the VPN client file to a selected directory.

Step 3 Unpack the file using the **zcat** and **tar** commands. For example:

```
zcat vpnclient-linux-x.x.x-K9.tar.gz | tar xvf -
```

(where x.x.x is the version number)

This command creates the vpnclient directory in the current directory.

Installing the Software

Before you install a new version of the VPN client, or reinstall your current version, you must use the **stop** command to disable VPN service.

If you are upgrading from the VPN 5000 client to the VPN client, use the following **stop** command:

```
/etc/rc.d/init.d/vpn stop
```

If you are upgrading from the VPN 3000 client to the VPN client, use the following **stop** command:

```
/etc/rc.d/init.d/vpnclient_init stop
```

To install the VPN client for Linux

Step 1 Obtain superuser privileges to run the install script.

Step 2 Enter the following commands:

```
cd vpnclient
./vpn_install
```

Step 3 At the prompt, choose a directory in which to install the VPN client.

Use the default directory (by pressing Enter), or choose a directory in your user's path.

Step 4 Enable the VPN service by using one of the following methods:

- Reboot your computer.
- Enable the service without rebooting. Enter the following command:

```
/etc/rc.d/init.d/vpnclient_init start
```

About the VPN Client for Linux Install Script

During the installation process:

1. The module is compiled, linked, and copied to either the directory /lib/modules/preferred/CiscoVPN, if it exists, or to /lib/modules/*system*/CiscoVPN, where *system* is the kernel version.
2. The application binaries are copied to the specified destination directory.
3. The startup file /etc/rc.d/init.d/vpnclient_init is created to enable and disable the VPN service.
4. The links /etc/rc3.d/s85vpnclient and /etc/rc5.d/s85vpnclient are added to run level 3 and run level 5 if startup at boot time is requested.

   These links allow the tunnel server to start at boot time and run in levels 3 and 5.

User Profiles

This chapter describes how to create a VPN client user profile. A user profile is a list of configuration parameters that determine the connection entries for a remote user.

There are two ways to create a user profile:

- Use a text editor to modify the sample profile that comes with the VPN client installer and rename it.
- Create a unique user profile using a text editor.

User profiles have a .pcf file extension and reside in the default location /etc/CiscoSystemsVPNClient/Profiles/ directory.

There is only one user profile per connection.

Tip User profiles for the VPN client for Linux are interchangeable with user profiles from other platforms.

Contents

This chapter includes the following sections:

Sample Profile

The VPN client software comes with a sample user profile. The file is named sample.pcf.

The following is an example of a sample user profile that might come with your installer.

```
[main]
Description=sample user profile
Host=10.7.44.1
AuthType=1
GroupName=monkeys
EnableISPConnect=0
ISPConnectType=0
ISPConnect=
ISPCommand=
Username=gawf
SaveUserPassword=0
EnableBackup=0
BackupServer=
EnableNat=0
CertStore=0
CertName=
CertPath=
CertSubjectName=
CertSerialHash=00000000000000000000000000000000
DHGroup=2
ForceKeepAlives=0
```

Modifying the Sample Profile

To modify the sample profile

Step 1 Using a text editor, open the sample user profile.

Step 2 Modify the parameters you want to change.

See your administrator for IP addresses, user name, and any security information.

Step 3 Save your new profile with a unique name in the /etc/CiscoSystemsVPNClient/Profiles/ directory.

When you use the **vpnclient connect** command to establish a connection, use your new profilename.

User Profile Parameters

You can create your own user profile from scratch using any text editing program. Save your new profile in the /etc/CiscoSystemsVPNClient/Profiles/ directory.

At a minimum, you need the following parameters listed in your profile:

- [main]
- Host
- AuthType
- GroupName
- Username

See your administrator for IP addresses, user name, and any security information.

Table 3-1 describes the list of parameters that can be in a user profile.

Table 3-1 User Profile Parameters

Parameter	Description
[main]	This keyword is required and is used to identify the main section. Enter exactly as shown as the first entry in the user profile.
Description = *String*	This optional command describes this user profile. The maximum length is 246 alphanumeric characters.
Host = *IP_Address or hostname*	The hostname or IP address of the VPN device you want to connect with. The maximum length of the hostname is 255 alphanumeric characters.

Table 3-1 User Profile Parameters (continued)

Parameter	Description
AuthType = **{ 1 | 3 }**	The authentication type that this user is using. • **1** is preshared keys. • **3** is a digital certificate using an RSA signature. If you select **AuthType 1**, you must also configure the **GroupName** and **GroupPwd**.
GroupName = *String*	The name of the IPSec group configured on the VPN device that contains this user. The maximum length is 32 alphanumeric characters. This parameter is case-sensitive.
GroupPwd = *String*	The password for the IPSec group that contains this user. The minimum length is 4 alphanumeric characters. The maximum is 32. This parameter is case-sensitive and entered in clear text.
encGroupPwd = *String*	This parameter displays the group password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
Username = *String*	The name that identifies a user as a valid member of the IPSec group specified in **GroupName**. The VPN client prompts the user for this value during user authentication. The maximum length is 32 alphanumeric characters. This parameter is case-sensitive and entered in clear text.

Table 3-1 User Profile Parameters (continued)

Parameter	Description
UserPassword = *String*	This password used during extended authentication. If **SaveUserPassword** is enabled, the first time the VPN client reads this password, it is saved in the user profile as **encUserPassword**, and the clear text version is deleted. If **SaveUserPassword** is disabled, the VPN client deletes the clear text version of the user password in the user profile but it does not create an encrypted version.
encUserPassword = *String*	This parameter displays the user password in the user profile in its encrypted form. It is binary data represented as alphanumeric text.
SaveUserPassword = **{ 0 | 1 }**	Determines whether the user password or its encrypted form are valid in the user profile. • **0**, the default, displays the user password in clear text in the user profile and is saved locally. • **1** displays the user password in the user profile in its encrypted version, and the password is not saved locally. This value is set in the VPN device, not in the VPN client.
EnableBackup = **{ 0 | 1 }**	Specifies whether to use a backup server if the primary server is not available. • **0**, the default, disables the backup server. • **1** enables the backup server. You must also specify a **BackupServer**.

Table 3-1 User Profile Parameters (continued)

Parameter	Description
BackupServer = *IP_Address or hostname*	List of IP addresses or hostnames of backup servers. Separate multiple entries by commas. The maximum length of hostname is 255 alphanumeric characters.
EnableNAT = **{ 0 | 1 }**	This parameter specifies whether to enable secure transmission between a VPN client and a VPN device through a router serving as a firewall, which might also be using the NAT protocol. • **0**, the default, disables IPSec through NAT mode. • **1** enables IPSec through NAT mode.
ForceKeepAlives = **{ 0 | 1 }**	This parameter allows the VPN client to keep sending IKE and ESP keepalives for a connection at approximately 20-second intervals so that the port on an ESP-aware NAT/Firewall does not close. • **0**, the default, disables keepalives. • **1** enables keepalives.
PeerTimeout = *Number*	The number of seconds to wait before terminating a connection when the VPN device on the other end of the tunnel is not responding. The range is 30 to 480 seconds. The default is 90.
CertStore = **{ 0 | 1 }**	Identifies the type of store containing the configured certificate. • **0** = default, none. • **1** = Cisco.
CertName = *String*	Identifies the certificate used to connect to the VPN device. The maximum length is 129 alphanumeric characters.

Table 3-1 User Profile Parameters (continued)

Parameter	Description
CertPath = *String*	The pathname of the directory containing the certificate file. The maximum length is 259 alphanumeric characters.
CertSubjectName = *String*	The qualified distinguished name (DN) of the certificate's owner. You can either not include this parameter in the user profile or leave it blank.
CertSerialHash = *String*	A hash of the certificate's complete contents, which provides a means of validating the authenticity of the certificate. You can either not include this parameter in the user profile or leave it blank.
DHGroup = **{ 1 | 2 | 5 }**	Allows a network administrator to override the configured group value used to generate Diffie-Hellman key pairs on a VPN device. • **1** = modp group 1 • **2** = modp group 2 • **5** = modp group 5 The default is 2.

Using the Command Line Interface

This chapter explains how to use the VPN client's command line interface (CLI) to connect to a Cisco VPN device, generate statistical reports, and disconnect from the device. You can create your own script files that use the CLI commands to perform routine tasks, such as connect to a corporate server, run reports, and then disconnect from the server.

Contents

This chapter contains the following sections:

Displaying a List of VPN Client Commands

To display a list of available VPN client commands, go to the directory that contains the VPN client software and enter the **vpnclient** command at the command line prompt.

The following example shows the command and the information that is displayed.

```
%vpnclient
Cisco Systems VPN Client Version 3.0.7
Copyright (C) 1998-2001 Cisco Systems, Inc. All Rights Reserved.
Client Type(s): Linux
Running on: Linux 2.2.14-5.0 #1 Tue Mar 7 21:07:39 EST 2000 i686

Usage:
 vpnclient connect profilename [eraseuserpwd]
 vpnclient disconnect
 vpnclient stat [reset] [traffic] [tunnel] [route] [repeat]
```

Establishing a Connection

This section describes how to establish a VPN connection, what parameters you might need to enter, and how to manipulate the VPN Client window.

Note If you are connecting to a VPN device using Telnet or SSH, check to see if the device allows split tunneling. If it does not, you cannot access resources that are not tunneled.

To establish a connection, enter the following command:

```
vpnclient connect profilename
```

Profilename is the name of the user profile configured for this user (.pcf file). This parameter is required. Enter your profilename without the .pcf file extension. If your profilename contains spaces, enclose it in double quotation marks on the command line.

For more information on the profilename, see Chapter 3, “User Profiles.”

Depending on the parameters that have been configured in your user profile, you are asked for the following passwords:

- Group password
- User name
- User password

If your VPN client has been configured to use SecurID or RADIUS authentication, you are prompted for those passwords.

See your administrator for any security information.

The VPN Client window stays in the foreground when the connection is established to allow the VPN client to be reauthenticated during a rekey by the VPN device. To send the VPN Client window to the background, press **Ctrl-Z** followed by the **bg** command at the command line prompt.

Note If the VPN device you are connecting to is configured to support rekeying and you send the VPN Client window to the background, the tunnel disconnects when the first rekey occurs.

DNS Servers

The concentrator can be configured to send the IP addresses of DNS servers to the VPN client to use during tunnel sessions.

If the client receives the DNS server settings, it copies the file /etc/resolv.conf to a backup file /etc/resolv.conf.vpnbackup. When the tunnel closes, the original contents of /etc/resolv.conf are restored.

Viewing the Logging Files

This section describes how to capture and view logging information.

Note To view logging files, you must have logging enabled in the global profile (**EnableLog =1**) and the LOG class set. For more information on logging, see the "Global Profile Configuration Parameters" section on page 6-3.

To view the logging information, enter the following command:

```
/usr/local/bin/ipseclog /directory/clientlog.txt
```

To view the logging information in real time, enter the following command after you start the ipseclog:

```
tail -f /directory/clientlog.txt
```

The ipseclog does not automatically go to the background. To send the ipseclog to the background, press **Ctrl-Z** followed by **bg** on the command line, or enter the ampersand symbol at the end of the **view** command, as shown in the following example:

```
/usr/local/bin/ipseclog /directory/clientlog.txt &
```

If the ipseclog is in the background, you must bring it to the foreground before you end the VPN client application. To bring the ipseclog to the foreground, enter **fg** on the command line.

Disconnecting the VPN Client

This section describes methods for disconnecting the VPN client.

To disconnect from your session, use one of the following methods:

- Enter the following command:

  ```
  vpnclient disconnect
  ```

  The following example shows the command that disconnects you from your secure connection and the prompt you receive when you are not connected.

  ```
  vpnclient disconnect
  Disconnecting the IPSEC link.
  Your IPSec link is not connected.
  ```

- Press **Crtl-C** while you are in the VPN Client window.

Displaying VPN Client Statistics

This section describes the VPN client statistics command and the optional parameters to the command.

To generate status information about your connection, enter the following command:

```
vpnclient stat [reset][traffic][tunnel][route][repeat]
```

If you enter this command without any of the optional parameters, the **vpnclient stat** command displays all status information. The optional parameters are described in Table 4-1.

Table 4-1 Optional Parameters to the VPN Client Stat Command

Parameter	Description
reset	Restarts all connection counts from zero.
traffic	Displays a summary of bytes in and out, packets encrypted and decrypted, and packets discarded.
tunnel	Displays IPSec tunneling information.
route	Displays configured routes.
repeat	Provides a continuous display, refreshing it every few seconds. To end the display, press **Ctrl-C**.

Examples

This section shows examples of output from the different options for the **vpnclient stat** command.

The following is an example of information that the **vpnclient stat** command with no option displays.

```
vpnclient stat

IPSec tunnel information.
Client address: 209.154.64.50
Server address: 10.10.32.32
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000

VPN traffic summary.
Time connected: 0 day<s>, 00:18.32
Bytes out: 3420
Bytes in: 3538
Packets encrypted: 23
Packets decrypted: 57
Packets bypassed: 102
Packets discarded: 988

Configured routes
Secured   Network Destination    Netmask           Bytes
   *       10.10.32.32          255.255.255.255       7638
```

```
   *       0.0.0.0              0.0.0.0               1899
```

To reset all connection counters, use the **vpnclient stat reset** command.

```
vpnclient stat reset
Tunnel statistics have been reset.
```

The following is an example of information that the **vpnclient stat traffic** command displays.

```
vpnclient stat traffic

VPN traffic summary
Time connected: 0 day<s>, 00:30:04
Bytes out: 5460
Bytes in: 6090
Packets encrypted: 39
Packets decrypted: 91
Packets bypassed: 159
Packets discarded: 1608
```

The following is an example of information that the **vpnclient stat** tunnel command displays. The **vpnclient stat tunnel** command shows only tunneling information.

```
vpnclient stat tunnel

IPSec tunnel information.
Client address: 220.111.22.30
Server address: 10.10.10.1
Encryption: 168-bit 3-DES
Authentication: HMAC-MD5
IP Compression: None
NAT passthrough is active on port 5000
```

The following is an example of information that the **vpnclient stat route** command displays.

```
stat route

Configured routes
Secured   Network Destination    Netmask           Bytes
   *       10.10.02.02          255.255.255.255      17638
   *       0.0.0.0              0.0.0.0              18998
```

Managing Digital Certificates

This chapter describes how to manage digital certificates in your store for the VPN client using the command line interface. Your certificate store is the location in your local file system for storing digital certificates. The store for the VPN client for Linux is the Cisco store.

Contents

This chapter includes the following sections:

User Profile Keywords

To use certificates for authentication, you must have all keywords that apply to certificates correctly set in your user profile. Check your settings for the following keywords:

- **AuthType = 3** (certificate authentication)

- **CertStore = 1** (Cisco certificate store)
- **CertName = Common Name** (This must be the same common name that is entered for a certificate.)

See Chapter 3, "User Profiles," for more information on setting parameters in your user profile.

Command Line Interface

Digital certificate management is implemented using the command line interface.

The command line interface for certificate management operates in two ways:

- The standard Unix shell where you enter all arguments for a given command on the same line.

  ```
  cisco_cert_mgr -U -op enroll -f filename -chall challenge_phrase
  ```

- A prompting mode where you enter minimum arguments for a given command and are prompted for any remaining information.

  The minimum command line argument has the following basic form:

  ```
  cisco_cert_mgr -U -op operation
  cisco_cert_mgr -R -op operation
  cisco_cert_mgr -E -op operation
  ```

  where:

  - **-U** applies to the user or private certificate.

    You can use the -U flag for all certificate management command operations, except enroll_resume.

  - **-R** applies the root certificate or certificate authority (CA) certificate.

    You can use the -R flag for list, view, verify, delete, export, import, and change_password operations.

  - **-E** applies to certificate enrollment.

    You can only use the -E flag with list and delete, and you must specify it with the enroll_resume operation.

The **-op** argument is followed by the desired operation for the specified certificate. Valid operations for the certificate manager command are list, view, verify, delete, export, import, enroll, enroll_file, and enroll_resume. For more information on these operations, see the "Certificate Management Operations" section on page 5-5.

Certificate Contents

A typical digital certificate contains the following information:

- Common name–The name of the owner, usually both the first and last names. This field identifies the owner within the Public Key Infrastructure (PKI organization).
- Department–The name of the owner's department. This is the same as the organizational unit.
  - If you are connecting to a VPN 3000 concentrator, this field must match the **Group Name** configured for the owner in the concentrator.
  - If you are connecting to a VPN 5000 concentrator, this field must match the **VPNGroup-*groupname*** configured in the concentrator.
- Company–The company where the owner is using the certificate. This is the same as the organization.
- State–The state where the owner is using the certificate.
- Country–The two-character country code where the owner's system is located.
- Email–The email address of the owner of the certificate.
- Thumbprint–An MD5 hash of the certificate's complete contents. This provides a means for validating the authenticity of the certificate. For example, if you contact the issuing CA, you can use this identifier to verify that this certificate is the correct one to use.
- Key size–The size of the signing key pair in bits.

- Subject–The fully qualified distinguished name (DN) of the certificate's owner. This field uniquely identifies the owner of the certificate in a format that can be used for LDAP and X.500 directory queries. A typical subject includes the following fields:
  - common name (**cn**)
  - organizational unit, or department (**ou**)
  - organization, or company (**o**)
  - locality, city or town (**l**)
  - state or province (**st)**
  - country (**c)**
  - email address (**e)**

  Other items might be included in the Subject, depending on the certificate.
- Serial number–A unique identifier used for tracking the validity of the certificate on the Certificate Revocation Lists (CRLs).
- Issuer–The fully qualified distinguished name (DN) of the source that provided the certificate.
- Not before–The beginning date that the certificate is valid.
- Not after–The end date beyond which the certificate is no longer valid.

The following output is an example of the information contained in a digital certificate:

```
Common Name: Fred Flinstone
Department: Rock yard
Company: Stone Co.
State: (null)
Country: (null)
Email: fredf@stonemail.fake
Thumb Print: 2936A0C874141273761B7F06F8152CF6
Key Size: 1024
Subject:e=fredf@stonemail.fake,cn=Fred Flinstone,ou=Rockyard,o=Stone
Co. l=Bedrock
Serial #: 7E813E99B9E0F48077BF995AA8D4ED98
Issuer: Stone Co.
Not before: Thu May 24 18:00:00 2001
Not after: Mon May 24 17:59:59 2004
```

Password Protection on Certificates

Each digital certificate is protected by a password. Many operations performed by the certificate management command require that you enter the password before the operation can take place.

The operations that require you to enter a password are:

- Delete
- Import
- Export
- Enroll

Note For the enroll operation, the password to protect the digital certificate is a separate password from the optional challenge password that you enter for the server certificate.

You are prompted for any passwords that are needed to complete the command. You must enter the password and verify the password again before the command can take place. If the password is not accepted, you must reenter the command.

A certificate password is also required when you establish a VPN connection with a certficate.

All passwords can be up to 32 alphanumeric characters in length, and are case sensitive.

Certificate Management Operations

Certificate management operations are listed on the command line after you enter the minimum command line argument. Valid operation strings allow you to list, view, verify, delete, export, import, and enroll digital certificates in your store.

The following is an example of a certificate management command with the list operation, and a sample output.

```
cisco_cert_mgr -U -op list

cisco_cert_mgr Version 3.0.7

        Cert #          Common Name
          0             Fred Flinstone
          1             Dino
```

Table 5-1 describes the list of operations that can be used with the certificate management command.

Table 5-1 Certificate Management Operations

Operation	Description
list	Lists all certificates in the certificate store. Each certificate is preceded by a unique certificate tag (*Cert #)*, which is used to identify the certificate for a specified operation.
view -ct *Cert #*	Views the specified certificate. You must enter a certificate tag.
verify -ct *Cert #*	Verifies that the specified certificate is valid. You must enter a certificate tag. If the certificate is verified, you receive the message "Certificate *Cert #* verified". If the certificate fails verification for any reason, you receive the message "Certificate *Cert #* failed verification". Following this message is a text string which describes the reason for the failure.
delete -ct *Cert #*	Deletes the specifies certificate. You must enter a certificate tag.

Table 5-1 Certificate Management Operations (continued)

Operation	Description
export -ct *Cert #* **-f** *filename*	Exports the identified certificate from the certificate store to a specified filename. You must enter a certificate tag and a filename. If either is omitted, the command line prompts you for them. You must enter the full path of the destination. If you enter only the filename, the file is placed in your working directory.
import -ct *Cert #*	Imports a certificate from a specified filename to the certificate store. You must enter a certificate tag. This operation requires two different passwords:the password that protects the file (given by your administrator), and the password you select to protect the certificate.
enroll **-cn** *common_name* **-ou** *organizational_unit* **-o** *organization* **-st** *state* **-c** *country* **-e** *email* **-ip** *IP_Address* **-dn** *domain_name* **-caurl** *url_of _CA* **-cadn** *domain_name* **[-chall** *challenge_phrase***]**	Used only for user certificates. Obtains a certificate by enrolling with a CA over the network. You can enter each keyword individually on the command line, or enter the minimum command line argument with only the enroll operation and the command line prompts you for the required keywords. See the "Enrolling Certificates" section on page 5-9 for more information. You can obtain the challenge phrase from your administrator or from the CA.

Table 5-1 Certificate Management Operations (continued)

Operation	Description
enroll_file **-cn** *common_name* **-ou** *organizational_unit* **-o** *organization* **-st** *state* **-c** *country* **-e** *email* **-ip** *IP_Address* **-dn** *domain_name* **-f** *filename* **-enc [base64 | binary]**	Used only for user certificates. Generates an enrollment request file that can be emailed to the CA or pasted into a webpage form. When the certificate is generated by the CA, you must import it using the **import** operation. See the "Enrolling Certificates" section on page 5-9 for more information.
enroll_resume -E -ct *Cert #*	This operation cannot be used with user or root certificates. Resumes an interrupted network enrollment. You must enter the **-E** argument and a certificate tag.
change_password -ct *Cert #*	Changes a password for a specified digital certificate. You must enter a certificate tag. You must enter the current password before selecting the new password and confirming it.

Certificate Tags

A certificate tag is the identifier for each unique certificate. Some certificate management operations require that you enter a certificate tag argument before the operation can take place.

To enter a certificate tag argument, use the **-ct** command followed by the certificate identifier, listed as **-ct *Cert #*** next to the operation. The following example shows the **view** command with a required certificate tag:

```
cisco_cert_mgr -U -op view -ct 0
```

where the operation is **view**, and the certificate tag is **0**.

If you do not enter the **-ct** argument and certificate tag, the command line prompts you for it. If you enter an invalid certificate tag, the command line lists all certificates in the certificate store, and prompts you again for the certificate tag.

Operations that require certificate tags are listed in Table 5-1.

Enrolling Certificates

A Certificate Authority (CA) is a trusted organization that issues digital certificates to users to provide a means for verifying that a user is who they claim to be.

The enroll operation allows you to obtain a certificate by enrolling with a CA over the network. To use the enroll operation, you must be able to provide a list of personal information about the user. For a list of the information you need to provide with the enroll operation, see Table 5-2.

There are two operations that can be used in addition to the enroll operation: enroll_file and enroll_resume.

- The enroll_file operation generates an enrollment request file that can be emailed to a CA or posted into a webpage form.
- The enroll_resume operation resumes an interrupted network enrollment.

Enroll Operation

There are two ways to enter keywords for the enroll operation using the command line:

- Enter the certificate manager command and the enroll operation with the associated keywords on the command line as in the following example:

  ```
  cisco_cert_mgr -U -op enroll -cn Ren Hoek -ou Customer Service -o
  Stimpy, Inc, -st CO -c US -e ren@fake.fake -ip 10.10.10.10 -dn
  fake.fake -caurl http://192.168.0.32/certsrv/mscep/mscep.dll -cadn
  fake.fake
  ```

- Enter the minimum command line argument with the enroll operation and let the command line prompt you for each keyword entry.

The following example shows the prompts displayed by the command line when you enter the minimum command line argument with the enroll option:

```
cisco_cert_mgr -U -op enroll

cisco_cert_mgr Version 3.0.7

Enter Common Name (cn): Ren Hoek
Enter Department (ou): Customer Service
Enter Company (o): Stimpy Inc.
Enter your State (st): CO
Enter your Country (c): US
Enter your Email (e): ren@fake.fake
Enter your IP Address: 10.10.10.10
Enter your Domain Name: fake.fake
Enter the CA's URL: http://192.168.0.32/certsrv/mscep/mscep.dll
Enter the CA's Domain: fake.fake
Enter the Challenge Password:
```

Table 5-2 describes keywords for the enroll, enroll_file, and enroll_resume operations.

Table 5-2 Keywords for the Enroll Operation

Argument	Description
-cn *common_name*	The common name for the certificate.
-ou *organizational_unit*	The organizational unit for the certificate.
-o *organization*	The organization for the certificate.
-st *state*	The state for the certificate.
-c *country*	The country for the certificate.
-e *email*	The user email address for the certificate.
-ip *IP_Address*	The IP address of the user's system.
-dn *domain_name*	The fully qualified domain name of the user's system.
-caurl *url_of_CA*	The URL or network address of the CA.

Table 5-2 Keywords for the Enroll Operation (continued)

Argument	Description
-cadn *domain_name* **[-chall** *challenge_phrase* **]**	The CA's domain name. You can obtain the challenge phrase from your administrator or from the CA.
-enc [base64 | binary]	Select encoding of the output file. • **base64** is an ASCII-encoded PKCS10 file that you can display because it is in a text format. Choose this type when you want to cut and paste the text into the CA's website. • **binary** is a base-2 PKCS10 (Public-Key Cryptography Standards) file. You cannot display a binary-encoded file.

CHAPTER 6

Preconfiguring the VPN Client for Remote Users

A series of configuration parameters determine the user profiles that remote users choose to connect to a VPN device. These profiles have a .pcf file extension and the default location is /etc/CiscoSystemsVPNClient/Profiles.

There is also a global profile that you can use to set certain standards for all user profiles. The name of the global profile file is vpnclient.ini. You can create a global profile that contains preconfigured information for a group of users.

This chapter explains how to create and edit global profiles.

For information on user profiles, see Chapter 3, “User Profiles.”

Contents

This chapter contains the following sections:

Making a Parameter Read-only

To make a parameter read-only so that a user cannot change it within the VPN client applications, precede the parameter name with an exclamation mark (!). This only controls what the user can do *within* the VPN client applications. You cannot prevent someone from editing the global file or removing it.

Creating a Global Profile

The global profile, vpnclient.ini, resides in the /etc/CiscoSystemsVPNClient/ directory. This is the default location and is created during installation.

The following is an example of what a global profile looks like when you open it with a text editor.

```
[main]
RunAtLogon=0
EnableLog=1
[LOG.IKE]
LogLevel=1
[LOG.CM]
LogLevel=1
[LOG.PPP]
LogLevel=2
[LOG.DIALER]
LogLevel=2
[LOG.CVPND]
LogLevel=1
[LOG.CERT]
LogLevel=0
[LOG.IPSEC]
LogLevel=3
[CertEnrollment]
SubjectName=Alice Wonderland
Company=University of OZ
Department=International Relations
State=Massachusetts
Country=US
Email=AliceW@UOZ.com
CADomainName=CertsAreUs
CAHostAddress=10.10.10.10.
CACertificate=CAU
```

Global Profile Configuration Parameters

This section describes the parameters that can be configured in the global profile. Table 6-1 lists all parameters and their descriptions.

Table 6-1 Global Profile Parameters

Keyword	Description
[main]	This keyword is required and is used to identify the main section. Enter exactly as shown as the first entry in the user profile.
EnableLog = **{ 0 | 1 }**	Determines whether to override log settings for the classes that use logging services. By default, logging is turned on. Use this parameter if you want to disable logging without having to set the log levels to zero for each of the classes. • **0** disables logging services. • **1** enables logging services. You can improve the performance of the VPN client system by turning logging off.
BinDirPath = *String*	The path where the VPN client was installed. The maximum value is 512 characters. The default is /usr/local/bin.
LogLevel = **{ 0 | 1 | 2 | 3 | }**	Determines the log level for individual classes that use logging services. • 0 disables logging services for the specified [LOG] class. • 1, low, displays only critical and warning events. This is the default. • 2, medium, displays critical, warning, and informational events. • 3, high, displays all events.
Use the **LogLevel** parameter to set the logging level for each of the following LOG classes. Enter the parameter as shown.	
[LOG.IKE]	Identifies the IKE class for setting the logging level.

Table 6-1 Global Profile Parameters (continued)

Keyword	Description
[LOG.CM]	Identifies the CM class for setting the logging level.
[LOG.CVPND]	Identifies the CVNPD class for setting the logging level.
[LOG.CERT]	Identifies the CERT class for setting the logging level.
[LOG.IPSEC]	Identifies the IPSEC class for setting the logging level.
CACertificate = *String*	Identifies the name of the self-signed certificate issued by the certificate authority (CA). The maximum length is 519 alphanumeric characters.
NetworkProxy = *IP_Address or hostname*	Identifies a proxy server you can use to route HTTP traffic. Using a network proxy can help prevent intrusions on your private network. The maximum length of hostname is 519 alphanumeric characters. The proxy setting might have a port associated with it. If so, enter the port number after the IP address. For example, 10.10.10.10.8080.

Limiting User Access

Upon installation, any user on your system can establish a VPN connection, view, edit, and add user profiles. You can limit users from accessing certain files, and limit their ability to establish a connection.

To limit access to the VPN client to only the root user, issue the following commands:

```
% chmod 700 /usr/local/bin/vpnclient
% chmod 700 /usr/local/bin/cvpnd
% chmod 700 /etc/CiscoSystemsVPNClient/Profiles
% chmod 700 /etc/CiscoSystemsVPNClient/Certificates
% chmod 700 /etc/CiscoSystemsVPNClient/vpnclient.ini
% chmod 700 /etc/CiscoSystemsVPNClient/Profiles/*
```

To limit access to profile information but allow a VPN connection, issue the following commands:

```
% chmod 700 /etc/CiscoSystemsVPNClient/Profiles
% chmod 700 /etc/CiscoSystemsVPNClient/Certificates
% chmod 700 /etc/CiscoSystemsVPNClient/vpnclient.ini
% chmod 700 /etc/CiscoSystemsVPNClient/Profiles/*
```

To reset the VPN client and return the cvpnd, vpnclient.ini, profiles, and certificate directories back to default permissions, rerun the VPN install script. For more information on running the install script, see the "Installing the Software" section on page 2-2.

Distributing Preconfigured VPN Client Software

This section describes how to distribute the preconfigured VPN client profiles. You can distribute the VPN client global profile or user profile to users separately or as part of the VPN client software.

Separate Distribution

To distribute the profiles separately and have users import them into the VPN client after they have installed it on their PCs:

- Distribute the appropriate profile files to users on whatever media you prefer.
- Supply users with necessary configuration information.
- Instruct users to:
  - Install the VPN client according to the instructions in Chapter 2, "Installing the VPN Client for Linux."
  - Modify their user profile as described in Chapter 3, "User Profiles."
  - Establish a VPN client connection as described in Chapter 4, "Using the Command Line Interface."

Distributing VPN Client Software

If the vpnclient.ini file is bundled with the VPN client software, it automatically configures the VPN client during installation. You can also distribute the preconfigured user profile files (one .pcf file for each connection entry) for automatic configuration.

To distribute preconfigured copies of the VPN client software to users for installation:

Step 1 Copy the VPN client software files from the distribution CD-ROM into each directory where you created a global profile (vpnclient.ini) and separate user profiles (.pcf) for a set of users.

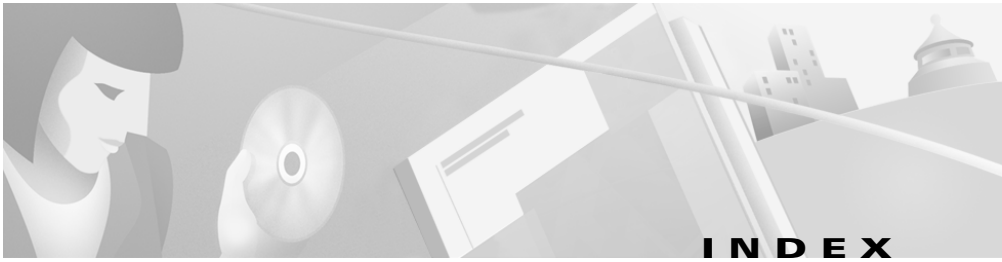
- Cisco Systems provides two images of the VPN client software files on the distribution CD-ROM:
  - CD-ROM image: Directory \VPN Client\CD-ROM. Use these files if users are installing the VPN client through a direct network connection.
  - Diskette image: Directories \VPN Client\Floppy\Disk1, ..\Disk2, and ..\Disk3. Use these files if users are installing the VPN client from diskettes. Copy the complete subdirectories to your system.

Step 2 Prepare and distribute the bundled software.

- For CD-ROM or network distribution:

  Be sure the vpnclient.ini file and profile files are in the same directory with all the CD-ROM image files. You can have users install from this directory through a network connection; or you can copy all files to a new CD-ROM for distribution; or you can create a self-extracting ZIP file that contains all the files from this directory, and have users download it, and then install the software.

- For diskette distribution:
  - Move the vpnclient.ini and profile files to the ..\Disk1 subdirectory.
  - Copy the files from the subdirectories onto three separate diskettes labeled Disk1, Disk2, and Disk3 for distribution to users.
  - Supply users with any other necessary configuration information and instructions.



A

B

C

D

E

F

G

H

I

K

L

N

O

P

R

S

T

U

V

Z